UNIVERSITÉ DE MONTRÉAL

MEASURES OF CRITICAL INFRASTRUCTURE VULNERABILITY TO DESTRUCTIVE EVENTS

LUCAS IULIANI

DÉPARTEMENT DE MATHÉMATIQUES ET DE GÉNIE INDUSTRIEL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

MÉMOIRE PRÉSENTÉ EN VUE DE L'OBTENTION

DU DIPLÔME DE MAITRISE ÈS SCIENCES APPLIQUÉES

(GÉNIE INDUSTRIEL)

DÉCEMBRE 2016

UNIVERSITÉ DE MONTRÉAL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

Ce mémoire intitulé :

MEASURES OF CRITICAL INFRASTRUCTURE VULNERABILITY TO DESTRUCTIVE EVENTS

présenté par : IULIANI Lucas

en vue de l'obtention du diplôme de : Maitrise ès sciences appliquées

a été dûment accepté par le jury d'examen constitué de :

M. JOANIS Marcelin, Ph. D., président

Mme DE MARCELLIS-WARIN Nathalie, Doctorat, membre et directeur de recherche

M. GALBRAITH John W., D. Phil., membre et codirecteur de recherche

M. SINCLAIR-DESGAGNÉ Bernard, Ph. D., membre

DEDICATION

"You should call it entropy, for two reasons. In the first place, your uncertainty function has been used in statistical mechanics under that name, so it already has a name. In the second place, and more importantly, nobody knows what entropy really is, so in a debate you will always have the advantage.".

—John Von Neumann

ACKNOWLEDGEMENTS

This graduate research would not have been possible if not for the guidance and encouragement of Professor John W. Galbraith. His sustained dedication—despite his many more pressing engagements and bloated inbox—was incredibly appreciated. May the end of this research mark the start of a new friendship. Here's to many coffees together in the future.

Special thanks are also due to Professor Nathalie de Marcellis-Warin, without whom my time in graduate school would not have been nearly as interesting or inspiring. The number of graduate students that gravitate towards her, eager to take part in her esearch and learn from her unique experiences, are a testament to her charisma and intellect.

Lastly, and most importantly, thank you to the family and friends at my back. Your patience, cheer, love and encouragement kept me typing during those slower days.

RÉSUMÉ

Les infrastructures critiques sont les actifs physiques qui fournissent aux sociétés modernes les services et besoins nécessaires pour le bon fonctionnement d'activités sociales et économiques essentielles. L'importance de ces infrastructures complexes est largement reconnue et la nécessité de protéger ces réseaux contre des événements destructifs—intentionnels ou accidentels—attire l'attention de plusieurs chercheurs et experts en sécurité. Il est également bien reconnu que le coût et les efforts associés à la protection totale représentent un énorme défi. La société réalisera son plus grand retour sur investissement en identifiant, en priorisant et en protégeant stratégiquement les actifs les plus vulnérables de son portefeuille d'infrastructures. Cela implique la nécessité d'une méthodologie de sélection permettant de cibler les actifs les plus cruciaux et de mesurer efficacement la vulnérabilité globale d'un réseau donné, ce qui nous permettra d'évaluer les niveaux de risque actuels et d'évaluer les améliorations techniques proposés. Le travail à suivre tente de mesurer la robustesse des systèmes d'infrastructures critiques en utilisant une approche basée sur les conséquences, évaluant la fonctionnalité de ces réseaux suite à la survenance d'un événement destructeur. Pour ce faire, des applications empiriques de deux approches différentes—une première utilisant la méthodologie fondée sur la théorie des réseaux et une deuxième méthodologie, proposé pour la première fois, fondée sur l'entropie—ont été réalisées sur les réseaux de transport d'électricité des quatre plus grandes provinces canadiennes en utilisant l'information disponible dans le domaine public.

Notre enquête sur les similitudes entre ces deux méthodologies distinctes n'a fourni aucune similarité définitive lors de la comparaison de la vulnérabilité des provinces, mesurée selon les différentes approches, mais a éclairée des avenues prometteuses pour de la recherche future.

ABSTRACT

Critical infrastructure systems are the physical assets that provide modern societies with the fundamental resources required to conduct essential economic and social operations, from power and electricity to drinking water and telecommunications. The crucial importance of these vast, complex and ubiquitous infrastructures is widely acknowledged and as such, the necessity to protect these networks from destructive events—both intentional and accidental—has garnered the attention of researchers and security experts alike. Similarly, it is also well recognized that the cost and effort associated with total protection presents an enormous challenge. Society will achieve its greatest return on investment by correctly identifying, prioritizing and protecting the most vulnerable assets in its infrastructure portfolio. This implies the need for a screening methodology by which we can target the most crucial assets, and effective metrics with which to gauge the vulnerability of a given network as a whole, allowing us to assess risk levels and evaluate proposed or completed engineering changes. The following work studies the robustness of critical infrastructure systems using a consequence-based framework, assessing the functionality of networks conditional on some destructive event having taken place. In order to do so, empirical applications of two different approaches—the network theory-based methodology and a novel entropy-based methodology—were carried out on the electrical transmission networks of the four largest Canadian provinces, using information available in the public domain.

Our attempt to investigate the similarities between the separate methodologies failed to provide any meaningful consistencies when comparing provinces' robustness according to the different grading schemes, but did provide promising avenues for future research.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS AND ABBREVIATIONS

A_G	Adjacency matrix of graph G
a_{ij}	Adjacency matrix value for nodes i and j
B_G	Incidence matrix of graph G
b_{ij}	Incidence matrix value for nodes i and j
b_i	Betweeness centrality of node i
c_i	Closeness centrality of node i
C	Clustering coefficient
CAS	Complex adaptive systems
CGE	Computable general equilibrium
CI	Critical infrastructures
D	Graph diameter
d_i	Node degree
d_G	Average degree
d_{ij}	Geodesic, or shortest path
δ_{ij}	Kronecker delta
E	Set of edges E
E_{glob}	Network efficiency
e_i	Individual edge
e_i	Eigenvector centrality of node i
G	Graph G
H	Entropy
k_i	Node degree
L	Average path length

L_i	Loss of supply resulting from destruction of site *i*
L^{-1}	Harmonic mean
M	System robustness
M	Meshedness coefficient
m	Network size
m_0	Entropy of sources
m_1	Re-scaled entropy of sources
m_2	Proportionate required capacity
n	Network order
π	Probability of new node connection to existing node
P	System reliability
p_i	Individual component reliability
R	System robustness
R	Total required supply
r_i	Remaining proportion of required supply
r	Assortativity coefficient
S	System resilience
$\sigma(\rho)$	Connectivity loss after removal of ρ fraction of nodes
V	Set of vertices V
v_i	Individual vertex
V	System vulnerability
X	Total supply available
x_i	Individual sources of supply

LIST OF APPENDICES

CHAPTER 1 INTRODUCTION

The developed world relies on the rapid, reliable and inexpensive delivery of goods and services. Each day, billions of dollars in trade are secured onto cargo ships and make their way across the globe, navigating the ocean's network of shipping lanes to their final port of delivery. Deep beneath the surface, fiber optic cables spanning the distances between continents provide virtually all of the world's reliable means of telecommunications, such as the Internet. This Internet service in turn goes on to help supervise, control and automate many of the supply chains that make up our utilities infrastructures, such as natural gas or oil pipelines and power grids. Together, these systems have been optimally designed and operate in tandem in order to provide the fundamental resources that keep our economies moving and societies functioning.

While the efficiency of these economic arrangements is among the primary focus areas of economic research, it is reasonable to ask whether improvements in productivity, delivery or overall efficiency have been accompanied by changes in vulnerability of output to catastrophic events. These crucial structural elements underlying economic activity may be affected by destructive events such as extreme weather, accidents or terrorist activity. In fact, there have been a number of documented examples in which economic activity at the level of a city has been severely disrupted by such events. While we cannot measure all the elements relevant to the robustness of economic activity, it is reasonable to assume that we can characterize the robustness of systems whose failure has been responsible for major economic disruptions in the past. Put simply, if we can measure the robustness of these crucial infrastructure elements, we will have some insight about the robustness of the broader economy that depends on them.

1.1 Critical infrastructure systems

Critical infrastructures (CI) are the physical assets that supply modern societies with the goods and resources required to perform everyday economic and social activities. This definition can be understood to include individual sectors of basic economic activity, such as power, energy, water distribution, telecommunications and others, as well as the individual components that make up these complex systems, such as dams, pipelines, utilities grids, radio towers, etc. In this contemporary globalized and interconnected environment, we can safely assume that our

increased reliance on critical infrastructure systems, coupled with their sprawling growth and continued degradation, gives rise to a potentially unprecedented level of vulnerability.

The importance of these infrastructures has long been understood. In Presidential Executive Order 13010, issued in July 1996, President Bill Clinton stated that "Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire and rescue), and continuity of government" (Executive Office of the President, 1996). Naturally, other nation states in the developed world grapple with similar technological risks.

More detailed lists of these essential assets have since been proposed, grouping together individual CI sectors into prioritized tiers which attempt to reflect the logical and functional dependencies between sectors, in that the outputs of certain processes provide the inputs to others (Lewis, 2006).

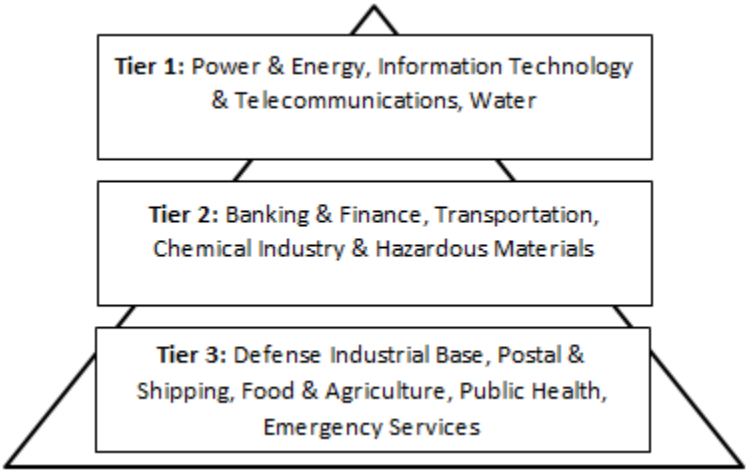


Figure 1.1: Prioritized list of critical infrastructure sectors

Additionally, it has become common practice in modern policy and academic research to include lists of Key Assets alongside summaries of CI sectors. As defined in the 2003 National Security Strategy for the Physical Protection of Critical Infrastructures and Key Assets, Key Assets are the individual physical targets or "high profile events" whose attack could result in large-scale causalities and destruction, but also "profound damage to […] national prestige, morale and confidence" (Department of Homeland Security, 2003). While, individually, certain physical Key

Assets such as dams and nuclear power plants may not be vital to the continuity of critical services, a successful attack may incur significant loss of life or other long-term, adverse public health and safety concerns. Other Key Assets such as national monuments, historical attractions and icons are said to hold “symbolic” value, and their destruction would result in the decline in the public’s moral and sense of safety and wellbeing.

Executive Order 13010 went on to highlight the need for cooperation between the public and private sectors in the development of a strategy for the protection of the critical assets, given that the bulk of these infrastructures are both owned and operated by private industry. In fact, it is estimated that 85% of all CI assets within the United States are held and managed by private business (Brown, Carlyle, Salmerón, & Wood, 2005). As it will become clear in subsequent sections, the information required for the development and implementation of protection methodologies makes the cooperation between government and industry necessary.

1.2 Threats to critical infrastructure

Lastly, and perhaps most importantly, President Clinton established a framework describing the two categories of threat vectors which present risks to CI systems: physical threats and cyber threats. Physical threats are the more conventional vectors that put at risk the integrity of tangible property, while cyber threats are the “threats of electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures.”

1.2.1 Physical threats

Physical threats to critical infrastructure are those that cause damage to tangible assets. This definition includes both intentional acts—such as vandalism, sabotage and terrorism—as well as unintentional damage caused by malfunction, natural hazards and technological or industrial accidents. While there may exist certain similarities in the overall outcomes of both hazards and directed attacks, the main distinction is the presence of an intelligent and ill-intention actor, aiming to achieve maximal loss of life or social disruption. It is therefore straightforward to assume that the damage caused by studied and directed attacks will generally cause greater disruption than those caused by the randomness of accidental and undirected events. Any accurate modeling or simulation technique should reflect this.

When considering physical threats to CI systems, non-state actors who view attacks on critical infrastructure as a means of achieving various political or ideological objectives are generally the object of greatest concern. In fact, well known terrorist organizations have advocated such attacks for years. An al-Qa'ida training manual, seized by the Manchester Metropolitan Police during a 2003 raid, notes as its primary mission the "overthrow of godless regimes [by] gathering information about the enemy, the land, the installations, and neighbours [and] blasting and destroying places of amusement, embassies, vital economic centers [and] bridges leading into and out of cities" (United States Air University, 2003).

Energy infrastructure in particular has a long history of being viewed as high-value targets for violent non-state actors. Information compiled by the Energy Infrastructure Attack Database (EIAD) has shown that there were, on average, 400 annual attacks carried out on energy infrastructures over the 2003-2013 timeframe (Giroux, 2013). Given their vital economic importance, striking these assets makes for an effective means of airing grievances and adversely impacting economy and security while garnering international media coverage. The vastness of the infrastructures, which can span long distances, provides a sizeable attack surface, contributing to their attractiveness. The raiding and ensuing hostage crisis at the Tigantourine natural gas facility in Amenas, Algeria in January 2013 was among the most high-profile of such events.

A more recent example of politically-motivated attacks directed at energy infrastructure is the November 2015 sabotage of major electrical transmission towers by anti-Russian activists, which caused blackouts affecting 2 million people over several days in Crimea. Here, the objective was not loss of life, but rather a protest of the region's annexation weeks earlier.

Assuring the physical security of CI systems is a challenging endeavour given the expansiveness of these infrastructures, and the cost associated with methods limiting access to them, such as underground installations, fencing, barricading, other hardening and physical surveillance.

1.2.2 Cyber threats

The rise of cyber security concerns, in the realm of CI protection as in all others, is characteristic of the 21st century international security landscape. And while the term "cyber threats" is typically used to include criminal activities such as fraud, espionage and theft broadly, it is used

here in reference to all electronic, radio-frequency or computer threats directed at control and communication CI networks and subsystems.

As with physical threats, defending against cyber attacks is made difficult by the enormity of the attack surface at which opponents may take aim. This phenomenon was in part enabled by the modernization of industrial processes and the growing trend towards the adoption of digital technologies.

A notable cyber-attack target in the case of CI systems is the industrial control and automation technologies employed throughout many different sectors. These electrical subsystems are used in the automated operation of industrial process equipment, such as machinery (boilers, pumps, valves, etc.) and electrical components (switches, interrupters, variable frequency drives, etc.). The use of industrial control systems obviously provides massive gains in efficiency, speeding up reaction time, automating changes in processes and limiting human intervention and error. Unfortunately however, it also provides hackers with well-known points of access.

The Stuxnet computer virus, now the world's most infamous cyber weapon, was built with the purpose of targeting and subverting industrial control equipment. Believed to have been jointly developed by American and Israeli intelligence and defence agencies, the computer worm infiltrated the programmable logic controllers (PLCs) used as part of the Iranian nuclear program. Once embedded in the Iranian network, the weapon gathered data on the industrial processes taking place before commanding fast-spinning centrifuges to overrun and self-destruct over time. Perhaps most impressively, the bug did so while displaying normal conditions to the system operators. Studies into the implications of the Stuxnet virus on the security of industrial controls systems have indicated that the worm may be used as a template for future intrusions in various sectors (Karnouskos, 2011). In the case of the Iranian nuclear program, it is believed that Stuxnet was introduced into the target environment via an infected external multimedia device, such as a USB flash drive. However, there exist alternative points of entry which may be exploited in order to gain access to closed networks.

One such alternative is the direct tampering of industrial control components. In his book *At the Abyss*, Thomas C. Reed, former Secretary of the U.S. Air Force and advisor to President Ronald Reagan, claimed that in 1982, the United States successfully inserted malicious software into control equipment purchased by the Soviet Union through Canadian suppliers. When deployed,

the software commanded the pumps and valves installed on a section of a Trans-Siberian gas pipeline to produce pressures exceeding design specifications, resulting in what Reed called “the most monumental non-nuclear explosion and fire ever seen from space.”

Connections to external networks such as the Internet—commonly used as a method of information and data communication—provide yet another point of access for hackers.

The level of sophistication required in the execution of such cyber-attacks leads experts to believe that the implication of state sponsors is required. As more sophisticated and subversive offensive capabilities are developed, the use of cyber-attacks is likely to become an interesting instrument of war for nation states, given the difficulty with attributing blame. While other overt means of coercion such as blockades and sanctions have long existed, cyber-attacks directed at economic interests provide a politically convenient form of economic warfare.

1.3 Critical infrastructure protection

In seeking to defend against physical and cyber threats to critical infrastructure, the cost—financial and social—associated with absolute protection is neither feasible nor desirable. The physical hardening of every last electrical distribution pylon or inch of pipeline does not represent a realistic engineering challenge, and the transformation of modern societies into police states, where barricades and armed guards are posted at every asset of value, is an equally unattractive outcome. Effective attempts at protecting critical infrastructure therefore rest on the careful prioritization and targeted defense of the most crucial assets of a given system. There exist various diverging approaches to assessing the importance of assets included throughout the associated literature. Broadly speaking, diverging asset prioritization schemes are divided along the two ends of the risk assessment spectrum.

Traditional probabilistic risk assessments seek answers to three fundamental questions: What can go wrong? How likely is it to go wrong? How bad would it be if it did? Mathematically,

$$Risk = P * C$$

where P is the probability of an unwanted or adverse event occurring and C, the associated negative impact. Risk, as defined above, is distinct from its usual meaning in economic or financial contexts, where it values likelihood of deviation from an expected return or macroeconomic condition. Within engineering frameworks, risk estimates expected loss. As

such, efforts at measuring the level of risk—or vulnerability—of a given system must therefore make assessments with respect to the variables above, either attempting to predict the likelihood of failure or quantifying the negative consequences of a given event taking place. Again, the associated literature provides diverging opinions on the two distinct approaches.

1.3.1 Reliability theory

A more traditional approach at addressing the problem of CI protection is contained in the engineering literature in the form of reliability engineering. Reliability engineering is concerned with the probabilistic estimation of component functionality or, inversely, its likelihood of failure, in an effort to characterize the reliability of systems as a whole. Reliability engineers, for instance, study the dependability or availability of physical assets, which is to say their functionality over a given period of time or at a specific point in time, respectively.

A system is said to have failed once it no longer provides a specified level of performance. Overall system performance is necessarily conditional on component functionality, and different measures of reliability can be considered for serial components and parallel components.

A serial system is one in which an input passes through each of a number of components in sequence, such that each one must be functioning for the system to function. Conversely, a parallel system is one in which an input may pass through any one of a number of components, such that only one of the components needs to be functioning for the system to function. Here, we use P to denote the reliability of a system and let p_i, $i = 1,2, \dots N$ denote the reliability of each of the N components of the system. For a serial system with independent probabilities of component reliability,

$$P = \prod_{i}^{N} p_i \qquad (1)$$

whereas for a parallel system with independent probabilities of component reliability, reliability is equal to 1 minus the probability of all parallel elements failing, such that

$$P = 1 - \prod_{i}^{N} (1 - p_i) \qquad (2)$$

As most real world systems are often composed of both serial and parallel elements, overall reliability can be computed from the individual reliabilities of the serial or parallel components.

While estimating reliability is valuable in the context of a physical structure such as the electricity grid—for example, in the scheduling of preventative maintenance efforts—there are several reasons why this approach may be insufficient in characterizing the vulnerability of large complex systems. First, actual failure probabilities may be difficult to characterize. The probability of an earthquake or other natural disaster, for example, is very difficult to estimate accurately. Second, some destructive events of the type that interest us may not be well characterized by probability distributions, as they result from deliberate acts of sabotage or terrorism. Lastly, the probability of failure of a system is only one quantity that we want to discover. We are also interested in the level of functionality that remains following some destructive event and component failure.

1.3.2 Resilience

As the problem of critical infrastructure vulnerability has gained interest in recent years, the concept of resilience has become a prominent approach to assessing the risk of both assets and supply chains, but also broader communities and economic sectors.

As a recent field of study, the idea of resilience has continued to evade a single canonical definition, with researchers prioritizing different aspects of the risk spectrum, and choosing to measure resilience according to diverging approaches. A recent publication from the Argonne National Laboratory entitled *Resilience: Theory and Applications* provides comprehensive overview of the varied literature on the topic, including both definitions and metrics (Carlson et al., 2012).

As the authors demonstrated, many studies have defined resilience as the ability of a system to recover from the adverse consequences of a disruptive event. However, such definitions fail to acknowledge the effects of preventative actions taken in order to reduce the likelihood or impact of a possible catastrophic event. Taking anticipative actions into account, resilience can be defined as: “the ability of an entity—e.g. an asset, organization, community, region, etc.—to anticipate, resist, absorb, respond to, adapt to and recover from a disturbance.”

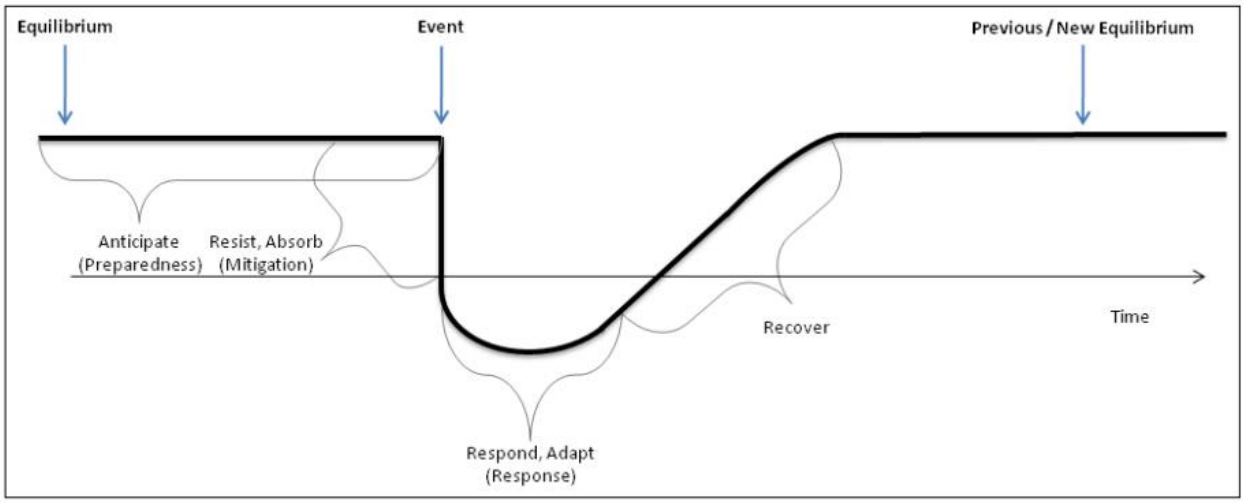


Figure 1.2: Aspects of Resilience and the Timing of an Adverse Event

The text goes on to highlight the importance of having a sound methodology for the measurement of asset/facility resilience, given its implications on the resilience of the broader system. Table 2 below provides Argonne's framework for understanding how the four fundamental resilience-enhancing measures—preparedness, mitigation, response and recovery—contribute to a given asset's overall resilience.

Table 1.1: Relationship between Aspects of Resilience and Resilience-Enhancing Measures

Anticipate	Resist	Absorb	Respond	Adapt	Recover
Preparedness	**Mitigation**		**Response**		**Recovery**
Activities taken by an entity to define the hazard environment to which it is subject.	Activities taken prior to an event to reduce the severity or consequences of a hazard.		Immediate and ongoing activities, tasks, programs, and systems that have been undertaken or developed to manage the adverse effects of an event.		Activities and programs designed to effectively and efficiently return conditions to a level that is acceptable to the entity.

The most frequently cited metric of both component and system resilience is time. More specifically, resilience engineers and analysts are concerned with the delay between the initial disruptive ent and the return to normal operations, or *Time to Recovery*. For example, a recent literature review published by the United States Environmental Protection Agency presented generic time-based resilience assessments applicable to water distribution networks. These metrics, presented in (Attoh-Okine, Cooper, & Mensah, 2009), (Ayyub, 2014) and others, compute resilience as a function of time ($Q(t)$). Resilience (S) can be tracked and measured as:

$$S = \frac{\int_{t_0}^{t_1} Q(t)dt}{100(t_0 - t_1)} \qquad (3)$$

where t_0 is a time before the hazardous event, and t_1 is a time after the event. The above equation allows for a variety of metrics to be used for $Q(t)$, so long as the variable used is affected by both the initial disruptive event and the restorative measures undertaken.

As with reliability, measures focused on resilience provide worthwhile insights as to the vulnerability of systems. Perhaps most importantly, time-based resilience measures allow system operators to gauge the impact of failures on end-users, and on how to best allocate capital in order to reduce delays until return to normal operations. In fact, for certain CI sectors, such as financial services and emergency response, it is clear that time-based measures provide the most worthwhile consequence assessments.

1.3.3 Robustness

Lastly, a final CI risk assessment approach is one that emphasizes the consequential aspect of the risk equation. As mentioned, while estimations of failure probabilities and recovery times are useful in the context of CI operations and emergency preparedness, we are also interested in the performance of CI systems conditional on a serious destructive event having taken place. Reliability and resilience engineering approaches prevent analysts and researchers from providing consequence-based vulnerability metrics that reflect the negative impacts of destructive events on end-users directly in terms of loss of supply.

There are a number of features that can limit the impact of a destructive event occurring within a given system. For instance, the adverse effect will tend to be less important if another part of the system can directly replace the output of the affected components. Similarly, the impact will be lower if the destructive event can be localized to the portion of the system in which it arose, such that the error propagation is limited. The same can be said for systems where damaged components can easily be replaced, or where neighbouring components can be adapted quickly. Any adequate measure of system robustness should capture these elements.

Broadly speaking, robust networks or systems are described as those that tolerate faults (Schuster, 2008) and provide low performance variation when conditions are perturbed (Gaury & Kleijnen, 1998). The notion of engineering design geared towards the reduction of performance

sensitivity to variation in conditions, as opposed to the pursuit of eliminating variation altogether, is attributed to Taguchi, for example in (Taguchi & Clausing, 1990). These definitions and features of robust system design have become commonly accepted throughout substantial engineering literatures (Sussman, 2008).

In the following work, we adopt robustness as a measure of remaining capacity and output following destructive events, arguing that variability of supply provides the most insightful and generalizable measure of CI vulnerability. Naturally, a complete understanding of a network's tolerance to component breakdown requires insights into its physical configuration, including vulnerable points such as bottlenecks, production sites and redundant features, as well as its inherent supply and demand dynamics.

1.4 Research objectives

The following research aims to contribute—however modestly—to the ongoing scientific efforts dedicated to the protection of critical infrastructure networks, using robustness as the measure of overall system vulnerability. Given the vastness and complexity of these systems, we recognize that theoretical and practical advances in both critical asset prioritization and overall system risk assessment methodologies are required to maximize society's efforts and return on investments. Understanding how to best prioritize and defend these infrastructural elements is the aim of this research paper, and our objectives towards achieving this goal can be described thusly:

a. to compare—at a theoretical level—network-based measures (a prominent approach to CI protection) with measures based directly on loss of output, such as entropy-based measures;
b. to determine whether these measures tend towards similar conclusions, despite valuing different aspects of overall CI system functionality, and;
c. to determine empirically whether any substantial differences can be seen when applying these two different approaches to the same real-world systems, and if so to try to interpret these differences.

As such, the subsequent paper is organized in order to convey an understanding of recent scientific advances in the field of CI protection and an exploration of its potential for future improvement.

Chapter 2 presents a critical overview of the current CI modeling and analysis methodologies, as they appear throughout the current cadre of academic and professional research, including economic, agent and system dynamics-based approaches. This literature review is continued in Chapter 3, which focuses solely on network theory-based methods of critical asset prioritization and system vulnerability assessment. Chapter 4 presents a novel approach to the challenge of CI protection, drawing from the field of information theory. Lastly, Chapter 5 is the paper's chief original contribution, and presents an empirical application of the network and information-theory based methodologies by evaluating the vulnerability of the electrical transmission networks in Canada's four largest provinces—British Columbia, Ontario, Alberta and Quebec—before concluding with a comparative analysis of the benefits and drawbacks of these two main approaches.

CHAPTER 2 LITERATURE REVIEW

Given their scope and complexity, the development of modeling and simulation methods is often seen as a prerequisite to the real-world design, maintenance, operation, improvement or protection of CI systems. The following section reviews the existing models proposed throughout the CI literature and broadly groups the current schools of thought into three categories: economic theory-based approaches, agent-based approaches and system dynamics-based approaches. Rather than providing a complete and in-depth overview of existing methods, this section is intended to serve as an introduction by highlighting the fundamentals, applications, strengths and weaknesses of available and ongoing research. It should also be noted that the literature review is continued in the subsequent chapter, which is dedicated to network science and provides a more substantive summary of the field's relevant applications. As the reader will come to understand, empirical applications analyzed later in this work rely on the fundamentals of graph theory and may benefit from a more in-depth introduction to its main tenants and recent advances.

2.1 Economic theory-based approaches

Economic models generally seek simulate the behaviours of principal economic actors including households, producers, government regulators and other decision makers as they exchange goods, services and other resources. Such models can be useful in the modeling of critical infrastructure systems, in that the actions of such stakeholders—producers, consumers and operators—are critical in the proper functioning of balanced and optimal infrastructures. Below, we present the fundamentals and recent advances for two distinct economic modeling approaches: Input-Output models and Computable General Equilibrium models.

2.1.1 Input-Output models

The Input-Output economic model was first submitted by Nobel laureate Wassily Leontief in 1951 (Leontief, 1986). The quantitative framework he proposed depicted inter-relations among different industry sectors for a given region, showing how output from one industrial sector may become an input to another. The model comes together in the form of matrix, where n sectors of an economic model are considered as variables of a set of linear equations, with each sector i producing a single good x_i. It is assumed that producing a single unit from sector i requires a_{ij}

units delivered from sector j and that interdependency between sectors forces them to produce and consume outputs mutually, while also satisfying a demand d_i. The output of sector i becomes:

$$x_i = a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_x + d_i \qquad (4)$$

By defining A as the matrix of coefficients a_{ij}, x as the vector of total output and d as the vector of aggregate demand, the expression for a complete economy becomes:

$$x = Ax + d \qquad (5)$$

Following basic re-formulation, it becomes clear that, given a reversible $(I - A)$ matrix, the model is a linear system of equations with a unique solution. With a known final demand d, the required output can be found.

While the application of the Input-Output (IO) model is widespread, its use in the field of critical infrastructure protection is relatively recent. Its first adaptation for the study of failures or *inoperabilities* was originally proposed by Haimes and Jiang (Haimes & Jiang, 2001). Where the traditional IO model was concerned with n sectors and i resources, their infrastructure model considered a system of n critical complex intraconnected and interconnected infrastructures, with the output being their risk of inoperability that can be triggered by one or multiple failures due to complexity, accidents, or acts of terrorism. Inoperability is defined as the inability of a system to complete its intended function, measured in this instance as a continuous variable between 0 and 1, with 0 representing complete functionality and 1, complete failure. In keeping with the established Leontief model, the Inoperability Input-Output model (IIM) can be formulated as:

$$x = Ax + c_k = (I - A)^{-1}c_k \qquad (6)$$

where x_j, $j = 1,2,\dots,n$, is the overall risk of inoperability of the complex intraconnected and interconnected jth infrastructure; a_{kj} is the probability of inoperability that the jth infrastructure contributes to the kth infrastructure due to the complexity of their interconnectedness and c_k the additional risk of inoperability that is inherent in the complexity (i.e., intraconnectedness) of the kth critical infrastructure. As highlighted above, and assuming $(I - A)$ is non-singular, the system of equations can be solved for the overall risk of inoperability of the infrastructures x.

As with the fundamental Leontief model on which it is based, a series of refined IIM models have subsequently been proposed. The *demand-reduction IIM* defines perturbations as the reduction of aggregate demand for a set of economic sectors in response to an event, and afterwards deduces the output reduction or inoperability of each involved interdependent economic sector (Santos & Haimes, 2004). *Dynamic IIM* refines the traditional model by integrating resilience coefficients for individual economic sectors (Lian & Haimes, 2006). *Multiregional IIM* expands the scope of the original model by including multiregional interdependencies based on the use of geospatial datasets (Crowther & Haimes, 2010).

Advocates of IIM-based modeling often highlight the intuitive interpretations of interdependencies offered by its different variations. Other major strengths of interoperability models are their accuracy in forecasting high-level error propagation among interconnected infrastructures and their insight as to effective mitigation efforts. These models also benefit from widely available existing datasets at both national and regional scales, such as the Bureau of Economic Analysis's *Benchmark Input-Output Data* database, thereby facilitating their application. Often-cited applications of IIM-based models include studies of the financial effects of the US Northeast blackout of 2003 (Anderson, Santos, & Haimes, 2007), the catastrophic impact of US Gulf hurricanes in 2005 (Crowther, Haimes, & Taub, 2007), the resilience of telecommunications systems and power distribution infrastructure in the aftermath of Hurricane Katrina (Reed, Kapur, & Christie, 2009) and the effects of September 11th on the global airline industry (Santos, 2006).

The IIM models are, however, not without their weaknesses. While necessary input data is readily available, these datasets reflect the interdependency of sectors during normal economic operations, ignoring real-time infrastructure or industry outputs. IIM-based approaches fail to analyze the interdependencies that exist at the component level, providing instead a snapshot of aggregate for a given economic sector.

2.1.2 Computable General Equilibrium models

Computable General Equilibrium (CGE) models are often viewed as an improvement of the I-O models proposed by Leontief, as they possess the same fundamental features—such as the interdependency of economic sectors—but overcome several of its limitations, such as including the linearity of these interdependencies, and address the lack of behavioral responses to

fluctuations in market resources and prices (Rose, 1995). Within CGE models, producers' production functions are modified to incorporate economic resilience, allowing for substitution analysis in cases of disruptions to normal market conditions due to external perturbations.

Several recent studies focused on CIS have used CGE as a means to estimate economics losses following disturbances, and to measure the effectiveness of proposed or implemented mitigation efforts.

Notably, work by Rose et al. analyzed the economic impacts of a hypothetical terrorist attack on the power distribution system of the city of Los Angeles. Economic losses were initially estimated at $20.5 billion, but reduced to $2.8 billion following the proposed (theoretical) implementation of various mitigation strategies, such as energy conservation, de-centralized onsite electricity generation and rescheduling of production (Rose, Oladosu, & Liao, 2007).

As with traditional $(I - O)$ models, the limitations of CGE models are that they provided a high-level, macroeconomic snapshot of the economy, at a discrete point in time and do not offer any insight as to component-level interdependencies or consequences of failure.

2.2 Agent-based approaches

Complex Adaptive Systems (CAS) are also considered among the most promising areas of research pertaining to the modeling of critical infrastructure systems. Within the theoretical CAS frameworks, different components—or *agents*—which have been programmed into a model according to a prescribed set of rules, interact together in ways that continuously remodel future outcomes. Each agent is said to be an entity with distinct location, capability and memory (Gell-Mann, 1994). The agent-based approach in the study of CAS adopts a bottom-up method and posits that complex behavior or phenomenon arises from many simple and individual interactions (Kaegi, Mock, & Kröger, 2009). This *emergent* behavior is characteristic of CAS models. Typically, CAS applications in the study of CIS use idealized networks (e.g. small-world networks) to represent infrastructure systems and components whose interdependencies are governed by empirical rules (Dueñas-Osorio, 2005). Perhaps most notably, CAS agent-based models have emerged as the preferred method of CIS modeling for several national laboratories and research centers within the United States.

In the late 1990s, the Sandia National Laboratories, whose chief mandate under the United States Department of Energy is the engineering and testing of non-nuclear components of the country`s nuclear weapons arsenal, developed their first full-scale CAS model. Dubbed *Aspen*, the model aimed to simulate the behaviors of a large number of individual economic decision-makers at a high level of detail. While imperfect, the model's outputs in reaction to federal monetary policies provided a detailed analysis of the financial sector, including the banking sector and bond market (Basu, Pryor, & Quint, 1998). In December 2000, an improvement of the original model, titled *Aspen-EE* (Electricity Enhancement), was Sandia's first attempt at modeling infrastructure interdependencies, with a focus on the electric power system, and included agents representing power markets and their reaction to power outages (Barton, Eidson, Schoenwald, Stamber, & Reinert, 2000). For both *Aspen* and *Aspen-EE*, the models proposed represented interactions between sectors, players and assets as so-called message-passing mechanisms, rather than modeling physical infrastructures themselves. A later model, *CommAspen*, was released in 2004, extended and modified the previous models by accounting for the telecommunications systems and its effect on the previously studied banking, finance and power networks (Cox, Barton, Reinert, Eidson, & Schoenwald, 2004). That same year, the *N-ABLE* model was published, this time integrating households and economic firms into the model as an added layer of detail (Eidson & Ehlen, n.d.) and in 2008, Sandia went on to study the specific threat of cyber-attacks on basic physical assets (Kelic, Warren, & Phillips, n.d.).

A second federal research center run by the United States Department of Energy, the Argonne National Laboratory, developed its first agent-based CIS model, the *Spot Market Agent Research Tool Version 2.0*, in 2000. Unlike models previously developed by Sandia at that time, *SMART II* took into consideration the physical layout—or *topology*—of power grids. Working closely with the Western Area Power Administration, one of the four power marketing administrations of the U.S. Department of Energy, Argonne's model was capable of detecting the transmissions line configurations which would most likely lead to spikes in prices and therefore contribute to greater market price stability (M. J. North, 2001). An extension to the original model, called *SMART II++*, was later developed, adding natural gas marketing and distribution agents to the simulations. These individual infrastructures were then coupled together, in the form of gas-fired electricity generators, in order to allow for interdependency analysis (M. J. N. North, 2000). Completed simulations demonstrated the need to intelligently monitor the purchase of natural gas

destined for energy production, so as to avoid power network failures from cascading into the natural gas infrastructures.

Lastly, the Idaho National Laboratory proposed their first CIS modeling approach, called the *Critical Infrastructure Modeling System*, in 2006 (Dudenhoeffer, Permann, & Manic, 2006). The CIMS tool used 3D graphical representations of CIS components and their interdependencies in order to anfalyze potential cascades and consequences of their potential failures. In contrast to the models developed by their peers, *CIMS* modeled infrastructure topologies in great detail and provided decision makers with the ability to easily visualize these interdependencies and their consequences. It became clear to the developers however, that once CIS sizes and interdependencies became increasingly complex, visualization methods were no longer suitable for rigorous analysis.

Complex adaptive systems are ideal as a means to simulate critical infrastructure systems in that they allow for the modeling of various decision makers' behaviours, system interdependencies and the effectiveness of proposed control strategies. Perhaps most importantly, CAS can be used in tandem with other modeling techniques to provide a more complete understanding of systems and the consequences associated with their failures.

2.3 System dynamics-based approaches

Systems theory is the science of understanding *systems*—i.e. sets of individual components which interact to form complex processes and complete a specific function—at a conceptual level, and across a broad spectrum of social and technological fields. Systems dynamics is the subfield of systems theory concerned with understanding the behaviour of complex systems over time, using stocks, flows, feedback loops and time delays to model different nonlinearities (MIT, 2016). Stocks are variables which can be quantified at a specific point in time, while flows are variables measured per unit of time. Feedback loops are the name of component outputs which are routed back as inputs, forming a circular process. This so-called feedback is characteristic of the system dynamics approach, and is particularly relevant in the study of self-regulating or self-correcting systems.

Put simply, while the agent-based approaches described above attempt to model the decision-making mechanisms of system subcomponents, systems dynamics models are interested in the processes occurring between them.

Originally developed by Jay Forrester in the 1950s to describe the dynamics of organizations, system dynamics modeling today provides a relevant, "blank canvas" approach to the modeling of CI interdependencies (Forrester, 1971) The most notable and frequently-cited application of systems dynamics modeling to CI protection is the Critical Infrastructure Protection/Decision Support System (CIP/DSS), developed by (Bush et al., 2005). As described by the authors, the tool models the interactions and dynamics of both the individual components and whole systems, according to their interdependencies. For example, "repairing damage to the electric power grid in a city requires transportation to failure sites and delivery of parts, fuel for repair vehicles, telecommunications for problem diagnosis and coordination of repairs, and the availability of labor. The repair itself involves diagnosis, ordering parts, dispatching crews, and performing work."

The dynamics processes involved are modeled according to governing rules—e.g. differential equations—and the output metrics are often estimates of disruption to, say, health, economic or environmental effects.

A relevant application of the model is the analysis of Hurricane Katrina on critical infrastructures of Baton Rouge (Santella, Zoli, & Steinberg, 2011). In the study, authors provided a framework establishing the infrastructure systems which proved most resilient, offering policy and engineering avenues for improvement.

While the systems dynamics approach provides a flexible approach to CI modeling, an over-reliance on expert judgment and a failure to provide insights as to component-level performance render the model incomplete. As with CAS approaches however, systems dynamics models can easily be integrated into other modeling methodologies.

CHAPTER 3 NETWORK SCIENCE

Networks are intuitive structures with which to model the form and function of real-world systems and processes. From supply chains to financial institutions and disease transmission pathways, the number of systems involving the distribution of goods and services between individual components is seemingly endless. And while its list of applications is difficult to summarize, the study of network science as a scientific discipline is today defined along three main pillars of research.

First, considerable efforts are dedicated to the characterization of network structures. This subset of academic research relies heavily on the mathematics branch of graph theory and involves mapping out the physical configurations of complex networks with the specified aim of understanding how they emerge and develop over time. Advances in this field have led to network generation algorithms, which allow researchers to build and experiment with ideal synthetic networks governed by the same laws as their real-world social, technological or biological counterparts.

Second, considerable resources are dedicated to the analysis of networks and the processes occurring within them, using mathematical tools and statistical mechanics. Together with the first pillar of research, the tools developed arm the designers and operators working on these various complex systems with the analytic and predictive tools necessary to manage these networks, and provide insight as to their improvement and future development.

Lastly, once empirical information pertaining to such networks has been aggregated and characterized, it is reasonable to question the feasibility of the tools at hand, given the scale of data being treated and computing times of algorithms involved. The third school of research in network science devotes itself to the computational implementation of theoretical advances made in the field, addressing limitations in data mining, computing efficiency and data visualization techniques. This line of research is left to a different author, and will go unmentioned throughout this work.

The following section provides an overview of the school of thought called network science, including its history and fundamental theory, which is required in order to conduct a critical review of current network-based models in the field of CI protection.

3.1 Historical review

Any historical review of the discipline of network science begins with famed mathematician Leonard Euler's resolution of the classic Konigsberg Seven Bridges problem in 1736. The problem challenged thinkers to find routes around Konigsberg requiring travelers to cross each of the city's seven bridges only once. Euler's analysis of the problem was the first to reformulate the challenge so as to summarize it to include only the individual lands masses, represented as points, and the links (bridges) connecting them, as illustrated in the figure below taken from (Wikipedia, 2016).

Figure 3.1: Euler's simplification of the Konigsberg bridge problem

In his paper on the topic, Euler laid down the fundamentals of graph theory and definitively demonstrated that the stated problem could not be solved (Sachs, Stiebitz, & Wilson, 1988). Subsequent improvements in the field attempted to emulate Euler's approach, aiming to accurately model and understand the structure and dynamics of real-world networks.

Subsequent advances were not made until much later, as research into networks became common in the health, social and pure & applied sciences. As it will become clear throughout the following section, research into these real-world networks resulted in them now being considered as part of three separate camps—random networks, scale-free networks and small-world networks—each with unique characteristics.

Random networks, as their name suggests, are networks for which connectivity between a given set of nodes occurs according to a random process, or other fixed probability distribution. A first random network model was proposed by Edgar Gilbert and described a wiring process by which each possible edge for a given set of nodes occurs independently with a probability between 0 and 1 (Gilbert, 1959). A second model for random networks was published contemporaneously by mathematicians Paul Erdos and Alfred Rényi, and described a connectivity model for which all

graphs possible given a fixed set of vertices and edges were considered equally probable (Erdös & Rényi, 1959). A main limitation of the *ER model* however, given its Poisson degree distribution, is that it fails to reflect the characteristics of certain real-world networks of interest.

One such characteristic is the presence of certain highly-connected "hubs" within networks. This phenomenon results in a Power Law degree distribution, as opposed to a Poisson distribution, and has clear repercussions on the function and robustness on the concerned systems. Recent study into these so-called *scale-free networks* began with the mapping of the World Wide Web led by researcher Albert Barabasi (Barabási & Albert, 1999). The Internet's configuration, Barabasi noticed, indicated that certain key nodes within the system—presumably those performing essential functions—were disproportionality well connected when compared to others. Subsequent work demonstrated that this was true for a variety of complex biological, social and technological systems (Barabási, 2003). While previous models were composed of a fixed set of nodes and edges, Barabasi and Albert argued that these complex systems continue to grow over time and that new nodes would attach preferentially to pre-existing nodes of greater importance. To capture this selective growth pattern, the authors proposed a generative graph model, now known as the *Barabasi-Albert model*, where the probability (π) of a new node connecting to an existing node i depends on the degree k_i of that node, such that:

$$\pi(k_i) = \frac{k_i}{\sum_j k_j} \qquad (7)$$

where j represents all other pre-existing nodes (R. Albert & Barabási, 2002).

Finally, the Watts-Strogatz model, proposed in 1998, offered an algorithmic approach to building a final sub-category of graphs: *small-world networks*. As will be discussed below in greater technical detail, the small-world phenomenon was brought to prominence by social scientist Stanley Milgram in the now-infamous "six degrees of separation" experiment, and demonstrated that within certain networks, any two given nodes are connected by a characteristically sort path (Milgram, 1967). Watts and Strogatz produced a model that addressed certain limitations of previous random graph models, and consisted of a wiring process that interpolated between an *ER* attachment scheme and a regular ring lattice (a graph which is obtained by beginning with a circular graph consisting of a single cycle and connecting each vertex to its neighbors two steps away (Singer, 2016)) (Watts & Strogatz, 1998).

3.2 Fundamentals of network theory

A given network– or *graph*, as it is commonly referred to in mathematical literature– is a collection of dots, called *nodes* or *edges*, and lines, called *vertices*, interconnecting them. Let us consider $G = (V, E)$, any graph made up of vertices $V(G) = \{v_1, v_2, \dots, v_n\}$ and edges $E(G) = \{e_1, e_2, \dots, e_n\}$. The number of vertices for each graph is its *order*, noted n, and the number of edges its *size*, m. Each graph can be mathematically summarized by its *adjacency matrix A*, for which:

$$a_{ij} := \begin{cases} 1 & if\ v_i v_j \in E \\ 0 & otherwise \end{cases} \qquad (8)$$

Obviously, A is symmetric, as any edge between v_i and v_j is also an edge between v_j and v_i. Hence, $a_{ij} = a_{ji}$. Alternatively, graphs are often summarized by their *incidence matrix B*, for which:

$$b_{ij} = \begin{cases} 1 & if\ v_i \in e_i \\ 0 & otherwise \end{cases} \qquad (9)$$

A *path* is a sequence of vertices traversed by following edges from one to another across a network. Mathematically, it is a non-empty sub-graph $P = (V, E)$ of the form $V = \{v_0, v_1, \dots, v_k\}$ and $E = \{v_0 v_1, v_1 v_2, \dots, v_{k-1} v_k\}$ where all v_i are distinct (Dueñas-Osorio, 2005). The *length* of a path is the number of edges it traverses. The *distance* d_{ij}—or *geodesic path*— is the shortest path that exists between nodes i and j. If no such path is present, which is to say if i and j exist on different sub-graphs for which no physical link exists, $d_{ij} := \infty$. It is also important to note that distances need not be unique between nodes i and j, as two distinct paths may be of the same length.

Let us consider, for example, the graph G illustrated in Figure 1 below:

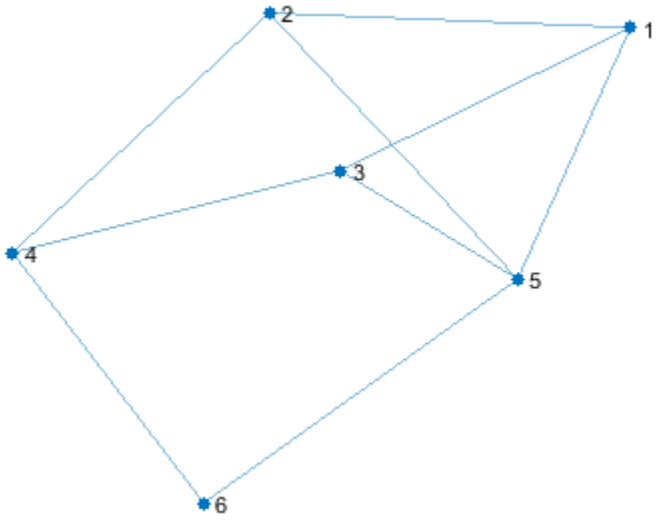


Figure 3.2: Graph G - an unweighted and undirected graph

It is made up of 6 vertices (or nodes) and 9 unweighted, undirected edges (or lines). Mathematically, $G = (V, E)$, where:

$$v_1 = 1$$
$$v_2 = 2$$
$$v_3 = 3$$
$$v_4 = 4$$
$$v_5 = 5$$
$$v_6 = 6$$

And

$$e_1 = (v_1, v_2)$$
$$e_2 = (v_1, v_3)$$
$$e_3 = (v_1, v_5)$$
$$e_4 = (v_2, v_4)$$
$$e_5 = (v_2, v_5)$$
$$e_6 = (v_3, v_4)$$
$$e_7 = (v_3, v_5)$$
$$e_8 = (v_4, v_6)$$
$$e_9 = (v_5, v_6)$$

Graph G can also be represented by its adjacency matrix A_G

$$A_G = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

as well as its incidence matrix B_G

$$B_G = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

In more detailed graphs, edges can be attributed values—or *weighted*—to characterize the processes taking place across the various arcs in question. In such cases, non-zero elements of the adjacency matrix can contain values other than 1, indicating *stronger* or *weaker* connections. A typical example of such weighted graphs is the flow or value of commodities being transited along elements of a supply chain. Similarly, *directed graphs*, are those which specify the direction of edges between vertices. Directed graphs can be represented by asymmetric adjacency matrixes for which $a_{ij} = 1$ or $a_{ij} = -1$ indicate an edge pointing in a direction specified by convention.

3.2.1 Network characterization

Characterizing networks allows us to gain an understanding of the physical configurations—or *topologies*—of different graphs. Using simple metrics as a means of describing graphs facilitates the comparison of different types of networks. The following section provides a brief overview of traditional parameters used in network characterization, as well as some of the most useful contemporary ones.

3.2.1.1 Average Path Length (L)

For undirected graphs, the average path length—sometimes referred to as mean distance—is defined as:

$$L = \frac{1}{\frac{1}{2}n(n+1)} \sum_{i \geq j} d_{ij} \qquad (10)$$

where d_{ij} is the shortest path—or *geodesic*—between vertices i and j. Average path length has been demonstrated to be particularly useful in its ability to indicate whether or not a given network exhibits so-called *small-world effect*. As first definitively observed throughout the course of several experiments during the 1960s by social psychologist Stanley Milgram, most pairs of vertices in most networks seem to be connected by a short path through the network. In the now-famous case of Milgram's research, letters passed from person to person were able to reach a designated target individual in only a small number of steps (six in the published case studies) (Milgram, 1967). Empirically, networks are said to exhibit this effect if the value of L scales logarithmically (or less) with n for a fixed average number of edges per vertex.

$$L \propto \log n$$

The emergence of so-called small-world effect within networks is therefore of considerable importance, as it pertains to the rapid delivery of goods—commodities, information, cash, etc.—from a source node to a delivery node.

In practice, computing average path length first requires solving the shortest path problem for a given network $G(V, E)$, from every node included in subset V to every other node. Computationally, this problem can be solved using Dijkstra's algorithm. Named after its creator, Edsger Dijkstra, the algorithm was first published in 1959, and proposed as an efficient method for the computation of the minimal total length between two nodes of a given graph (Dijkstra, 1959). It is the approach chosen for the calculation of d_{ij} in following subsections.

Lastly, we note that inverse average path length ($\frac{1}{L}$) is an often-cited and intuitive measure of the efficiency with which a resource can be delivered.

3.2.1.2 Harmonic mean (L^{-1})

In larger complex networks, which may contain disconnected sub-graphs, it is possible that any two vertices have no connecting path, and thus the calculation of mean distance becomes problematic. In such instances, the distance value would be defined conventionally as $d_{ij} := \infty$,

driving the *L* value to a meaningless infinity. A commonly used alternative is the *harmonic mean*, defined as (Newman, 2003):

$$L^{-1} = \frac{1}{\frac{1}{2}n(n+1)} \sum_{i \geq j} \frac{1}{d_{ij}} \qquad (11)$$

3.2.1.3 Diameter (D)

The diameter of a given network is the largest distance, measured in edges, between any two nodes in the network.

$$D = \max_{i,j} d_{ij} \qquad (12)$$

In the language of network theory, the diameter is the maximum shortest path between each pair of vertices. More practically, it represents the furthest possible distance that a given resource would need to travel in order to be delivered.

3.2.1.4 Degree (d_G)

Vertex degree is considered one of the most fundamental parameters in network theory. Mathematically, the degree of vertex v_i, denoted as d_i, is equal to the number of edges at v_i. The average degree d_G of a network is given by:

$$d_G = \frac{1}{n} \sum_{n \in G} d_i \qquad (13)$$

Or equivalently,

$$d_G = \frac{2m}{n} \qquad (14)$$

Average node degree serves as a basic measure for overall network sparseness. A sparse network is one for which the number of links m is less than the theoretical maximum number of links for that same network i.e. $m_{max} = n(n-1)/2$.

Moreover, it is intuitive to assume that a given node's level of connectivity provides a good measure of its importance within a network. Research in this area, for both ideal and real-world networks, has demonstrated that vertex degree is crucial in predicting a network's resilience to random and targeted attacks (Albert, Jeong, & Barabasi, 2000). A network's statistical

distribution of vertex degrees is in fact widely cited as a measure of network characterization. If a network's vertex degrees obey a Poisson distribution, displaying short thin tails, it has been demonstrated that it will be equally vulnerable to random or targeted attack, given that all nodes are of a typical degree i.e. level of connectivity. Alternatively, if a network's degree distribution follows a Power Law with long thick tails, indicating that a select number of nodes have disproportionately high degrees, it will show a considerable level of resilience to random disruptions and an increased level of vulnerability to targeted attacks.

3.2.1.5 Clustering coefficient (C)

The characterization of complex networks must necessarily seek to quantify the level of redundancy built into a given system, either by design or happenstance. As defined by Goulter, redundancy indicates the presence of "independent alternative paths between source and demand nodes which can be used to satisfy supply requirements during disruption or failure of the main paths" (Goulter, 1987).

Of these redundancy metrics, one of the most frequently used is the clustering coefficient, C, as first proposed by Barrat and Weigt (Barrat & Weigt, 1999). The clustering coefficient of a network indicates the average probability that two neighbors of a node are themselves adjacent by measuring the density of triangles—sets of three vertices for which each is connected to each of the others—within a given graph. As often paraphrased in the social sciences, C is the probability that "the friend of your friend is also your friend".

The clustering coefficient can be calculated by (Newman, 2003):

$$C = \frac{3 * number\ of\ triangles\ within\ the\ network}{number\ of\ connected\ triples\ of\ vertices} \qquad (15)$$

Here, a *connected triple of vertices* indicates a single vertex with edges connected to a pair of other vertices. In effect, C measures the ratio of "completed" *triples*, and the factor of 3 in the expression's numerator ensures that C lies in the range of $0 \leq C \leq 1$. C can also be expressed as:

$$C = \frac{6 * number\ of\ triangles\ in\ the\ network}{number\ of\ paths\ of\ length\ two} \qquad (16)$$

In the above expression, *a path of length two* refers to a directed path starting from a specified node. Alternatively, local measures of clustering have been proposed and can be measured as follows (Watts & Strogatz, 1998):

$$C_i = \frac{number\ of\ triangles\ connected\ to\ vertex\ i}{number\ of\ triples\ connected\ to\ vertex\ i} \qquad (17)$$

The clustering coefficient for an entire network, C, is then given as the mean of the network's local clustering coefficients (Newman, 2010):

$$C = \frac{1}{n}\sum_{i=1}^{n} C_i \qquad (18)$$

A graph with $C = 1$ is said to have maximal clustering, while one with $C = 0$ has no clustering. A common observation made of real-world networks is that they exhibit non-trivial clustering coefficients (Iyer et al., 2013).

We take for example, the graphs $A1$ and $A2$, illustrated in Figure 2 below, for which the clustering coefficients are 0 and 0.2, respectively.

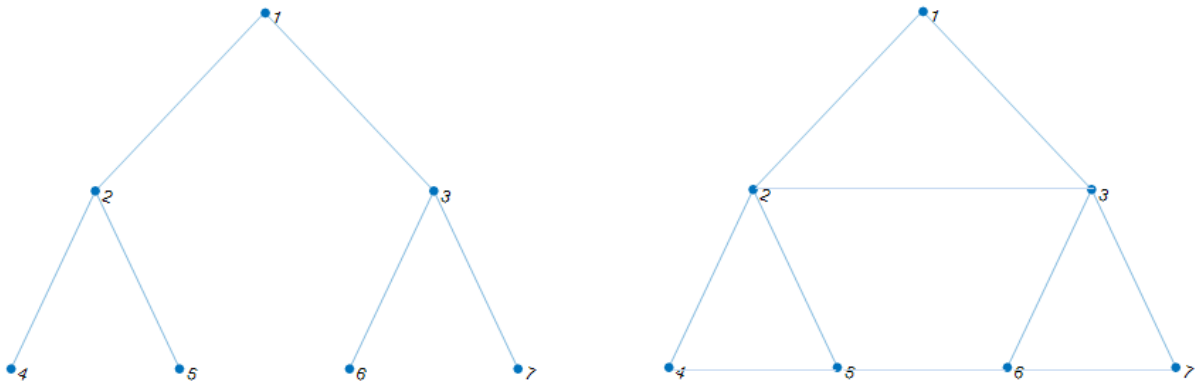


Figure 3.3: Graphs A1 and A2

While both graphs have similar topologies, we note the existence of edges (v_2, v_3), (v_4, v_5), (v_5, v_6) and (v_6, v_7) in graph *A2*. Let us consider a given scenario in which v_1 is a production node, nodes v_2 and $v_3$are transportation nodes and nodes v_4, v_5, v_6 and v_7 are delivery nodes. In such an example, these additional edges represent alternative transmission routes with which to deliver goods and services in the event of a hazard eliminating a single path. The operational

flexibility provided by the additional edges in graph $A2$ is reflected in the respective cluster scores.

This being said however, a noticeable limitation of the clustering coefficient is that it is a purely topological measure and ignores any edge capacity requirements. Additionally, it only provides information on triangular redundant loops.

3.2.1.6 Meshedness coefficient (M)

Given that the clustering coefficient presented above focuses on the identification of transitive triangles, an obvious extension of this metric would speculate as to level of redundancy present for loops of length four and above.

One such measure is the *meshedness coefficient, M*, originally proposed by Buhl (Buhl et al., 2006). When studying the spatial arrangement of urban settlements, the authors noted the typically low levels of clustering resulting from the typical parallel layout of roads in urban environments. In response, a novel coefficient for the measuring of "meshed" networks was proposed:

$$M = \frac{m - n + 1}{2n - 5} \qquad (19)$$

Similar to the clustering ratios, the meshedness coefficient measures network redundancy as a quotient of the number of actually present independent loops ($m - n + 1$) and the number of maximum possible loops ($2n - 5$). Here, M can vary from 0, for tree-structure networks, to 1, for complete planar graphs. It is interesting to note that M appears to be independent of network size, showing only very limited correlation to n.

Referring once again to graphs $A1$ and $A2$ illustrated in Figure 2 above, we note that their respective meshedness coefficients are 0 and 0.444. As with clustering, the alternative routes of delivery made possible by additional edges is reflected in the meshedness scores.

3.2.1.7 Network efficiency (E)

Network efficiency, as originally proposed by Latora and Marchiori, represents the ease with which any two vertices i and j can communicate and exchange information (Latora & Marchiori, 2001). It is defined as:

$$E_{glob} = \frac{1}{n(n-1)} \sum_{i \neq j \in G} \frac{1}{d_{ij}} \qquad (20)$$

where $0 \leq E_{glob} \leq 1$.

In the referenced paper, the authors proposed efficiency as an alternative to L in defining small-world behaviour is systems while dropping restrictions on unweightedness, connectedness and undirectedness. Networks with high efficiency are said to exhibit small-world behaviour.

Additionally, they viewed E_{glob} as a measure of *parallel* system efficiency, while the inverse of average path length ($\frac{1}{L}$) described the efficiency of *sequential* systems i.e. resources carried along a chain of components. Lastly, they described E_{glob} as a measure of system redundancy equivalent to the clustering coefficient, but with a very precise physical meaning: the efficiency in transporting information.

3.2.1.8 Assortativity coefficient (*r*)

A final often-cited characteristic of real-world networks is that they manifest some degree of assortativity or, conversely, disassortativity (Newman, 2002). In assortative networks, high degree nodes tend to be connected to other highly connected nodes and low degree nodes to other low degree ones. The opposite is true for networks which are said to be disassortative, where high degree nodes display a tendency to be connected to low degree nodes, and vice versa. The assortativity (or disassortativity) of a network with n nodes and m edges is measured by its assortativity coefficient, defined by:

$$r = \frac{\sum_{i,j=1}^{n} (a_{ij} - d_i d_j / 2m) d_i d_j}{\sum_{i,j=1}^{n} (d_i \delta_{ij} - d_i d_j / 2m) d_i d_j} \qquad (21)$$

where δ_{ij} is the Kronecker delta, such that

$$\delta_{ij} = \begin{cases} 0 \text{ if } i \neq j \\ 1 \text{ if } i \neq j \end{cases} \qquad (22)$$

Networks with $r > 0$ are assortative while networks with $r < 0$ are disassortative and those with $r = 0$ are neither.

As first demonstrated by Newman in the above-mentioned study, social networks are typically assortative, while biological and technological networks are usually disassortative.

3.2.2 Network Analysis

Understanding how networks continue to function once one or more of their component parts has been degraded is the chief objective in the study of network robustness. The process that results from the sequential removal of some fraction of a networks nodes and the study of its subsequent impact on the system's form and function is referred to as *percolation theory*, and is said to provide a natural model for studying the robustness of networked systems (Watts, Newman, Callaway, 2000). First proposed as a method for the study of the transmission of epidemics across social networks, percolation is commonly used today to study cascading failures across technological networks.

This approach implies the need for a preferential scheme with which to go about targeting nodes for removal. Moreover, given that a technological network's performance is intrinsically linked to its engineering design and boundary conditions, performance indicators are required in order to measure a system's functionally (or inversely, its level of degradation) as part of the continuous node-removal process. The following section provides an overview of the literature's most widely used centrality measures, as well as a set of proposed network performance indicators.

3.2.2.1 Centrality measures

Centrality measures attempt to identify the most central vertices within a network (Carrington, Scott, & Wasserman, 2005). While several of these measures have been proposed throughout the literature, here we focus on the four most common: degree centrality, betweeness centrality, closeness centrality and eigenvector centrality.

3.2.2.1.1 Degree centrality (d_i)

As highlighted in the previous chapter, a vertex's level of connectivity with its surrounding nodes provides a simple, yet effective measure of its importance within networks. This measure is a purely topological one and can be calculated using information contained in a graph's adjacency matrix A. A node's degree centrality is given by:

$$d_i = \sum_{j=1}^{N} A_{ij} \qquad (23)$$

The study of networks on this topic has demonstrated that degree centrality plays a large role in a network's survivability to random or targeted attacks (Albert et al., 2000). In the aforementioned research, authors studied the effect of node removal for two distinct networks: the infrastructure of the Internet and a 326,000-page subset of the World Wide Web. When targeting nodes at random, both networks displayed a high level of resilience when using remaining network connectivity as the chosen metric for robustness, which we address below. Removing nodes in order of the highest degrees was shown to have a devastating effect. If a network's vertex degree distribution is Poisson, with short thin tails, it will be equally vulnerable to random or targeted disruptions as each node will have a degree typical for the network. However, if the vertex degrees exhibit a Power Law distribution, with long thick tails, it will display significant resilience to random disruptions but a strong vulnerability to targeted attacks, as a select few nodes will have a disproportionately high level of connectivity. For any saboteur, terrorist or intelligent actor with ill intent, targeting nodes in decreasing order of degree would therefore seem like the most efficient method with which to cause maximum disruption

3.2.2.1.2 Betweeness centrality (b_i)

Betweeness centrality is a crude measure of the control a given node i exerts over the flow of commodities between others (Newman, 2003). It is calculated as the total number of shortest paths that traverse a given vertex i when the shortest paths are calculated between every pair of nodes (i, j) that exist in G, and for which i is not considered an end to any of the shortest paths (Borgatti, 2005). If we assume that goods are routed through the most direct path in a given infrastructure network, consistent with optimal engineering design practices, betweeness represents the total flow transiting through a given node i, and can be calculated as follows:

$$b_i = \sum_{s,t \in n} v_i(s,t) \qquad (24)$$

where

$$v_i(s,t) = \begin{cases} 1, if\ i\ lies\ on\ a\ geodesic\ path\ between\ s\ and\ t \\ 0\ , if\ otherwise \end{cases} \qquad (25)$$

It is interesting to note that a vertex may display a high level of betweeness while being connected to only a small number of other vertices. Such measures will allow us to correctly value the centrality of vertices that "bridge" together distant clusters of nodes. Here, we may

think of transmission lines of utilities infrastructures which often transport commodities across the long distances that bridge points of resource extraction or generation hubs and local distribution networks.

Let us consider, for example, network $B2$, illustrated in Figure 3 below. In this instance, we consider that vertices v_1, v_2, v_3 and v_4 are production nodes, v_5, v_6 and v_7 are distribution nodes and v_8, v_9, v_{10} and v_{11} are delivery nodes.

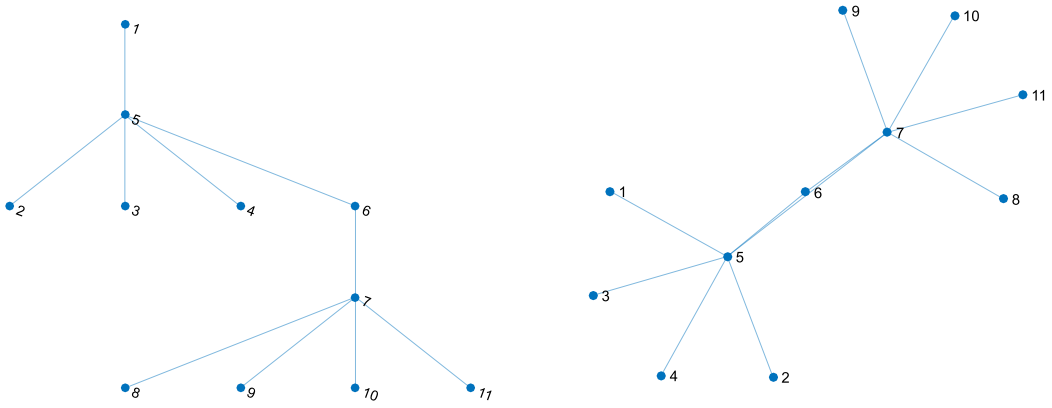


Figure 3.4: Graph B1and B2

We notice that when ordered according to their degree and betweeness centralities, the nodes of graph $B1$ are ranked identically.

Table 3.1: Degree and betweeness centrality rankings of graph B1

Degree	5	7	6	1	2	3	4
Betweeness	5	7	6	1	2	3	4

However, the same graph, modified to contain an additional edge joining nodes v_5 and v_7, as illustrated in graph $B2$, produces different rankings.

Table 3.2: Degree and betweeness centrality rankings of graph B2

Degree	5	7	6	1	2	3	4
Betweeness	5	7	1	2	3	4	6

While the rankings in terms of degree centralities remain unchanged, the addition of a new shortest path, providing a more optimal pathway for the delivery of resources from the

production hub at v_5 to the delivery terminal at v_7, is reflected in the ordering of nodes in accordance with betweeness centralities.

Perhaps most interestingly, is that while its input requirements demand no more than the topological information contained within a graph's adjacency matrix, betweeness centrality attempts to provide analysts with insight as to a network's flow transmission pathways, in accordance with common optimal engineering constraints. For those analysts concerned with the study of critical infrastructures, betweeness centrality would seem to provide an important tool with which to highlight chokepoints such as bottlenecks and crucial hubs.

3.2.2.1.3 . Closeness centrality

Closeness centrality provides a measure of importance based on the mean distance between any node and all other nodes in the network. The average distance of vertex i can be calculated as follows:

$$g_i = \frac{1}{n}\sum_{j \in n} d_{ij} \qquad (26)$$

where d_{ij} is the shortest distance (geodesic path) between nodes i and j. The closeness centrality of a given node is then calculated by:

$$c_i = \frac{1}{g_i} = \frac{n}{\sum_{j \in n} d_{ij}} \qquad (27)$$

Here, by calculating closeness centrality as the reciprocal of average distance, we ensure that high values are attributed to vertices that are a short geodesic distance from many other vertices in the network.

3.2.2.1.4 Eigenvector centrality

Eigenvector centrality can be viewed as a more refined version of degree centrality, as it based on the concept that a given node should be viewed as important if it is linked to nodes that are themselves important. First used by Philip Bonacich in 1972, the eigenvector centrality e_i of node i is defined as:

$$e_i = \frac{1}{\lambda}\sum_{j=1}^{n} a_{ij}e_j \qquad (28)$$

where λ is a constant (Bonacich, 1972). The above function can be rewritten in linear algebra notation as the eigenvector equation:

$$Ae = \lambda e \qquad (29)$$

While there may exist several different λ eigenvalues, the Perron-Frobenius theorem demonstrates that for a real square matrix with positive entries there exists a unique largest real eigenvalue for which the corresponding eigenvector, e, can be chosen to have strictly positive entries.

As with degree, betweeness and closeness, eigenvector centrality continues to be one of the most widely cited measures in a variety of social, biological and technological networks. In fact, Google's PageRank algorithm, used to gauge the importance of a given website, is a variant of eigenvector centrality.

3.2.2.1.5 Random node selection

Finally, in an effort to adopt an "all-hazards" approach to the problem of network (or critical infrastructure) vulnerability, the selection of nodes at random mimics the failure of components caused by natural hazards, aging and malfunction. It also provides a simplistic benchmark with which to gauge the effectiveness of previously mentioned intelligent node removal schemes.

3.2.2.2 Performance measures

The second requirement for the evaluation of system's robustness is the comparison of overall network functionality before and after a disruption (or an intelligent removal of nodes) has taken place. These performance indicators may capture network information on network topology alone, or can be refined to give an indication of flow pattern changes within the system being studied. The following section provides an overview of the measures typically used in percolation theory approaches.

3.2.2.2.1 Connectivity loss ($\sigma(\rho)$)

Connectivity loss is a purely topological measure of system performance. It studies how the size of the largest system component (i.e. sub-graph) will change as a fraction ρ of its vertices are removed. If, after the removal of a number of nodes, a network's remaining sub-graphs are sufficiently small, it is reasonable to assume that it will cease to meet its basic function requirements in any meaningful sense. For an initial network order n, we define n_ρ as the network resulting from the removal of ρ nodes according to a specified preferential scheme. The largest component of n_ρ will be n_ρ^c. Connectivity loss can then be calculated as:

$$\sigma(\rho) = \frac{\left|n_\rho^c\right|}{n} \qquad (30)$$

where $\left|n_\rho^c\right|$ is the number of vertices in n_ρ^c (Iyer, Killingback, Sundaram, & Wang, 2013). Measuring connectivity loss as a function of the fraction of nodes removed will allow for the plotting and comparison of different node-targeting approaches described in the previous subsection.

3.2.2.2.2 Network robustness (R)

While connectivity loss allows for the visualization of system functionality scaled by number of nodes removed, network robustness measures allow for the single-value quantification of a given network. The robustness of a network subjected to different types of vertex removal schemes can be valued according to (Schneider, Moreira, Andrade, Havlin, & Herrmann, 2011):

$$R = \frac{1}{n}\sum_{i=1}^{n}\left(\frac{i}{n}\right) \qquad (31)$$

The normalization factor of $\frac{1}{n}$ is used in order to compare the robustness of networks of different sizes. Also, it can be demonstrated that for any preferential vertex removal scheme, R attains a minimum value of $\frac{1}{n}$ and a maximum value of $\frac{1}{2}\left(1-\frac{1}{n}\right)$ (Iyer et al., 2013). As such, $R \in \left[0, \frac{1}{2}\right]$.

3.2.2.2.3 Network vulnerability (V)

The above-mentioned property of R has led to the use of its alternative value, network vulnerability, which can be valued as such (Iyer et al., 2013):

$$V = \frac{1}{2} - R \qquad (32)$$

3.2.3 Applications to critical infrastructure vulnerability

Graph theory provides a natural tool with which to represent the structure and dynamics of CI systems. In these models, nodes represent the individual components and links, the physical, logical and cyber dependencies between them. Additionally, weighted and directed edges can model flow capacities and delivery patterns, respectively.

Scholars attempting to estimate the vulnerability of networked systems using graph theory do so by studying a network's topology or flow, or both. Additionally, while some choose to focus on a given network class—for instance, power grids or oil pipelines—others are committed to the advancement of graph theory more broadly, and apply generic analytical methods to a variety of different technological networks.

Given their importance in the maintenance of economic and social functions, electricity grids have remained the focus of many studies aimed at assessing the vulnerability of largescale, complex networks.

Among such studies, the most widely-cited is the analysis of the North American power grid produced by (R. Albert, Albert, & Nakarado, 2004). The authors proposed a study of the structural vulnerability of the North American power grid, based on recent advances in the field of network theory. As highlighted in the text, "performing an analytic description of the electromagnetic processes integrated over the whole grid is a daunting, if not impossible, task" and as such, the authors recommended that power operators and security analysts rely instead on simplified models, which can be used to simulate deviations caused by external perturbations. Their model summarized the North American power grid as a network of 14,099 nodes (substations) and 19,657 edges (transmission lines). The authors attempted to demonstrate the degradation of network functionality based on the sequential targeting of different nodes, using a measure of connectivity loss to quantify the average decrease in the number of generators connected to a distributing substation, such that:

$$C_L = 1 - \left(\frac{N_g^i}{N_g}\right) \qquad (33)$$

where N_g is the number of generation stations (1,633 in total) and N_g^i, the number of generators connected to a given distribution node i following a disruption. In this form, connectivity loss measured the decrease of the ability of distribution substations to receive power from the generators. The study concluded that while the North American power grid displayed robustness to most perturbations, the targeting of key transmission substations in particular is what greatly reduced its ability to function and provide power to end users.

Another seminal work associated with the study of electrical transmission systems is the analysis of the Northwestern power grid produced by Duncan Watts and Steven Strogatz in 1998 (Watts & Strogatz, 1998). The authors demonstrated that, similar to other biological and social networks, the utilities grid under study exhibited small-world behaviour, with characteristic mean distances and non-trivial clustering ratios, and indicated a heightened risk of disease—or error, in the case of technological networks—propagation.

Network theory-based approaches have also been applied in measuring the robustness of the Internet to both random breakdown and targeted attacks. In (Cohen, Erez, ben-Avraham, & Havlin, 2000), the authors studied the resilience of the Internet to random breakdowns, noting that it, like many other large networks, followed a scale-free Power Law connectivity distribution. When removing, or "collapsing" nodes at random, it was demonstrated that the network exhibited a high degree of resilience to random breakdown, with "a cluster of interconnected sites spanning the whole Internet becoming more dilute with increasing breakdowns, but remaining essentially connected even for nearly 100% breakdown." In a subsequent work, the authors demonstrated that the same network was highly sensitive to intentional attack, when targeting nodes with high connectivity (R. Cohen, Erez, ben-Avraham, & Havlin, 2001).

CHAPTER 4 ENTROPY-BASED APPROACH TO ROBUSTNESS

The following section describes a model of system robustness based on the fundamentals of information theory, first presented in (Galbraith, 2009). As such, we begin by presenting the history and basic concepts of the information theory principles which we draw upon. Next, we present a novel approach to the measurement of system robustness. An empirical application of this model is then presented in Chapter 5.

4.1 Entropy-based model of robustness

Information theory is the branch of mathematics concerned with the study of how information can be quantified, transmitted and processed, and was first developed by famed mathematician Claude Shannon. While working as an engineer at Bell Laboratories in 1948, Shannon became interested with the problem of communicating information over a noisy channel, and sought out to develop a first empirical approach towards a scientific understanding of information. Shannon presented his findings in the seminal paper *A Mathematical Theory of Communication* (Shannon, 1948). In it, he describes the concept of "information" as a discrete set of possible messages, with the objective of communicating these messages to a receiver and having the receiver reconstruct the initial content with a low probability of error, despite noise present in the signal's channel.

Hence, the key measure of information described by Shannon is that of *entropy*, borrowed from the field of thermodynamics, where it was first developed by physicist Ludwig Boltzmann to characterize disorder within a given system, according to:

$$S = -k_B \sum_i p_i \, ln \, p_i \qquad (34)$$

where p_i is the probability of a given microstate i.e. a specific microscopic configuration of a thermodynamic system and k_B is the Boltzmann constant. In information theory however, entropy measures the amount of uncertainty of an unknown or random value, such that the entropy H of a random value is defined as:

$$H = -\sum_i p_i log_2 p_i \qquad (35)$$

Where H is measured in *bits* (as the base of the logarithm used here is 2), and p_i represents the probability of a given value occurring. To illustrate, we borrow the following practical example taken from (Ghahramani, 2006).

Let us suppose that we have been invited to a dinner hosted at a given apartment. We arrive at the designated building, comprised of 4 floors, each with 8 individual apartments, only to find that we have misplaced the host's apartment number. However, a neighbour exiting the building reminds us that the host lives on the fourth floor. By doing so, the neighbour has conveyed information, which is to say that he has reduced our uncertainty from 32 possibilities down to 8. If H is the variable describing in which apartment the event will be held, with equal probability for each apartment, it is initially calculated as $log_2(1/32) = -5$, where the entropy H is 5 bits. Once the neighbour informs us, the probability drops to 0 for the first 24 apartments, and to 1/8 for the remaining top-floor residencies. The entropy H then becomes 3 bits, and it can be said that the neighbour has conveyed 2 bits of information.

4.1.1 Properties of measures

As with the indicators proposed by graph theorists, an ideal measure of robustness (or vulnerability) would seek to consider both the structure of and dynamics occurring within a given system. Such a measure would reflect, for example, a network's output and production capacity, its bottlenecks and other single points of failure, as well as its required supply.

The following subsection will present examples of system structures as a preamble to subsequent discussion of numerical measures of robustness. In each case, the objective is to illustrate features needing to be captured by proposed metrics. We begin by presenting systems A and A' in the figure below.

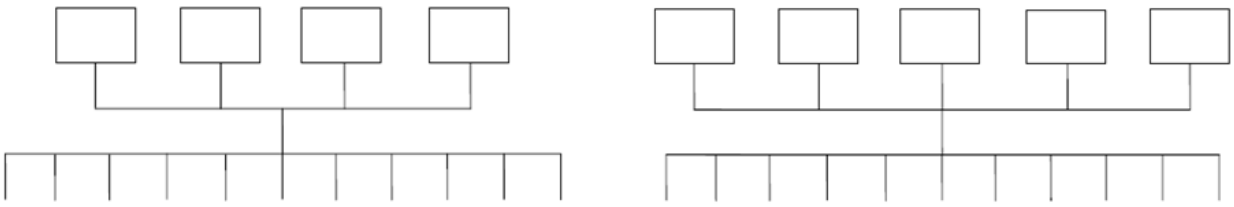


Figure 4.1: Example System Structures A and A'

In these examples, the required output (e.g. electricity, potable water, oil & gas products, food supply, etc.) is produced in the boxes and is transited along the channels to consumers at the bottom of the diagram. Here, we consider the production sites to be equivalent. These examples contain both serial and parallel elements, and given information regarding the failure probabilities of the various components, we could compute reliability measures for these systems. However, as discussed, our interest is not the dependability of a network during normal operating conditions, but rather its performance conditional on some destructive event having taken place.

While systems A and A' presented above differ in terms of the number of production sites, both have the property that all output passes through a single transmission channel. We might therefore wish to treat them as equivalent in terms of robustness, given that a single destructive event can eliminate all supply.

Case system B below is more robust in that the most damage a single destructive event can cause is the elimination of one of four sources of supply.

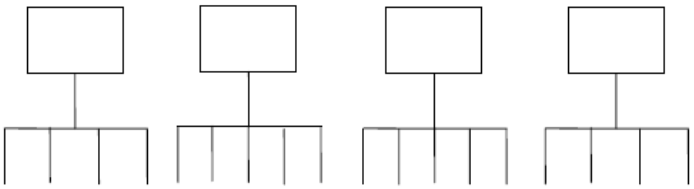


Figure 4.2: Example System Structure B

A valid numerical measure should therefore assign B a higher robustness value than A. We note, however, that B's sources cannot substitute for one another, as channels connecting the subsystems are nonexistent.

Case system C below has two sources of supply, and the end users supplied by each are again separated. This structure appears less robust than B but more robust than A.

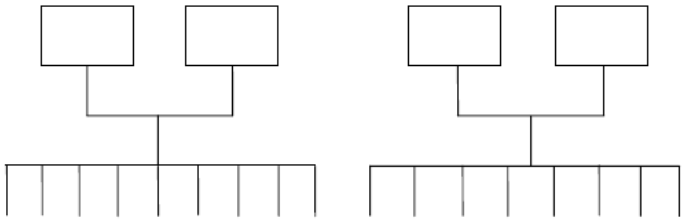


Figure 4.3: Example System Structure C

In both B and C, there are four production sites, but C's production sites are paired in passing through a single bottleneck, making the structure less robust. Two destructive events can end all output in C.

Case C' is similar in structure, but with two unequal sources. The network on the left groups together two production sites and the one on the right, three.

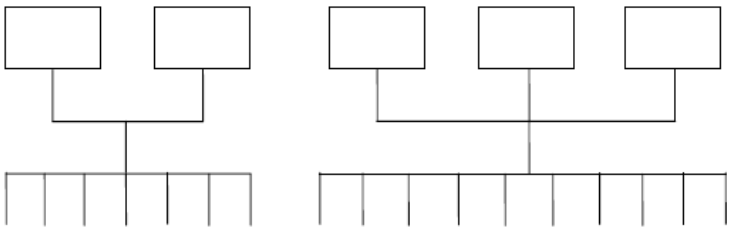


Figure 4.4: Example System Structure C'

The worst-case destructive event in case C' will then eliminate a greater quantity of supply to the end users than will the worst-case destructive event for case C. We might then assign C' a lower measure of robustness.

Finally, case D resembles case C in that it has two sources of supply, each of which consolidates two production sites.

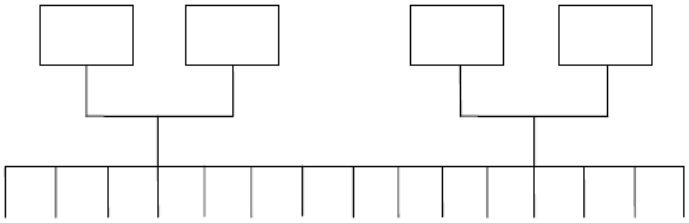


Figure 4.5: Example Structure System D

However, in case D, each source can supply any end user. If the supply is merely sufficient to meet baseline requirements, then we might deem D and C as equally robust, in that the worst destructive event in each case will eliminate half of the supply, and another could eliminate all. However, if the individual sources could each produce more than 50% of the requirement, D might be said to be more robust, given that the worst destructive event could eliminate either source, but the remaining one could supply more than 50% of end users with the required output.

Moreover, provided each source has enough excess capacity to meet all required output, then one source can be destroyed with no loss in output to end users.

Sensible measures of robustness should address each of these aspects: the number of sources, the total production capacity relative to requirement, and the bottlenecks defined as the minimal set of conduits through which all production passes.

Any ideal measure of system robustness should fulfill a few simple conditions. Let M be any measure of system robustness which is consistent with the following properties:

i. Monotonicity of supply: If an additional source of supply x_{N+1} is added to the system, M does not decrease.
ii. Monotonicity of bottlenecks: If the supply passing through any bottleneck is split between two or more bottlenecks, M does not decrease.
iii. Minimal robustness: If there is only one bottleneck i.e. if all output can be lost through destruction at one point, $M \equiv 0$.
iv. Dominance: If two systems A and B have the same structure and requirement R, but each source of supply in A is at least as great as the corresponding source of supply if B, and one source of supply in A is strictly greater than the corresponding source in $B, M_A \geq M_B$.
v. Scale invariance: If the outputs of all sources, and the total requirement R are changed in the same proportions within the same structure, M is unchanged.

4.1.2 Measures of robustness

Let us consider x_i number of index sources as defined previously, where $i = 1, 2, \dots, N$ and $x_i > 0 \forall i$. As such, $X = \sum_{i=1}^{N} x_i$ will be the total supply available and R the total required supply.

4.1.2.1 Entropy of sources

A first measure to consider, given that it is a commonly used measure of dispersion in analogous contexts, is entropy. In this case, we consider the simple entropy of sources of supply, such that:

$$m_0 = -\sum_{i=1}^{N} \left(\frac{x_i}{X}\right) \ln\left(\frac{x_i}{X}\right) \qquad (36)$$

We note that measure m_0 above requires no knowledge of total required supply, and uses only the total supply available. Similarly, although it measures dispersion, and is therefore related to the limitation of error propagation, it takes no account of any excess capacity or redundancy present in a given system. As such, entropy of sources will fail the monotonicity (i, ii), minimal

robustness (iii) and dominance (iv) properties described above, and fails to reflect the absolute level of output. For example, for a system with a given structure and required supply, outputs from three sources of 50, 50 and 50 will result in a higher entropy measure that outputs from three sources of 60, 70 and 80.

4.1.2.2 Re-scaled entropy of sources

A potential solution would to be adapt the simple entropy measure via non-negative re-scaling that takes levels of redundancy into consideration (implying that $X > R$), such that:

$$m_1 = m_0(\frac{X}{R}) \qquad (37)$$

Measure m_1, unlike m_0, can be shown to fulfill conditions i, ii and iv, as well as v. It does not, however, fulfill condition iii and also fails to capture the distinction between cases C and D given above. The fact that the supply system for some end users is cut off from that of others, limiting adaptability of the systems, is not captured by m_1.

In instances such as D, where this does not arise, as in typical city-level electrical grids or water distribution networks for example, m_1 may be sufficient. For other situations, we can define a third measure which would reflect this effect, but which also imposes higher informational requirements.

4.1.2.3 Proportionate required capacity

Such a measure would be based on the sum of the proportions of required capacity that remain after a sequence of destructive events, in line with the robustness definition discussed in Chapter 1. We begin by first defining measurements of a given network`s properties, which are necessary to calculate desired values.

Let the site of bottleneck 1 be the site that, if destroyed would lead to the single largest loss of output to end users. Let L_1 be the loss of supply that arises if this site 1 is destroyed and $l_1 = {L_1}/{R}$. Finally, we define $r_1 \in [0,1]$ as the proportion of required supply R that remains available to end users following such a destructive event. We note that in a system with excess capacity, we may have $r_1 = 1$ although $l_1 > 0$, which is to say that the loss incurred by destructive event 1

may be within the margin between requirement R and full capacity X. For a simple system such as D, for which production output can be delivered to any end user, we have:

$$r_i = 1 - [\frac{L_1 - (X - R)}{R}] \qquad (38)$$

In systems where $X = R$, then:

$$r_i = 1 - \frac{L_i}{R} = 1 - l_i \qquad (39)$$

In complex systems, establishing r_i will typically require careful study of the network structure.

Next, let bottleneck 2 be site which, if destroyed, would result in the largest loss of output to end users *given that site 1 has also been destroyed*. Let L_2 be the cumulative loss of output when both sites 1 and 2 are destroyed and let $r_2 \in [0,1]$be the proportion of requirement R that remains available following the described sequence of destructive events.

Continuing in this fashion, site k and L_k are respectively the kth most important site and the associated cumulative loss of output from the destruction of all bottleneck sites leading up to k inclusively. We define $l_k = {L_k}/{R}$ and r_k as the proportion of the total requirement R remaining after the k sequence of destructive events. We note that unless $X = R$, $r_k \neq 1 - l_k$. If $X > R$, then $r_k > 1 - l_k$ because some of the loss incurred is within the margin afforded by excess capacity.

We now propose a third measure which sums the remaining supplies after a sequence of destructive events up to N. As such, higher values indicate that more capacity remains, implying greater robustness.

$$m_2 = (\frac{X}{R}) \sum_{i=1}^{N} r_i \qquad (40)$$

We will have $r_i \in [0,1] \forall i$ and $r_N = 0$ where there are N bottlenecks. Measure m_2 requires greater input information that m_1, since we need the values of cumulative output losses, entailing information about the distribution network downstream of the sources of supply. Given this information, m_2 will allow for a more refined measure in cases where the distribution network is incompletely connected. As with m_1, scaling by ${X}/{R}$ allows us to capture the effect of a large

output from source 1, which would otherwise have no effect given that source 1 is eliminated in computing each term in the summation.

This third measure can also be shown to respect the previously listed conditions. Properties i and iv are respected, in that any additional source of supply cannot decrease r_i. Property ii is respected from the fact that the loss from the destruction of a bottleneck can be no less than the loss from the destruction of the two from which it could be split. If all output can be lost by destroying a single bottleneck, then $r_i = 0 \rightarrow m_2 = 0$. Finally, for property v, we note that $X/_R$ is unchanged since X and R change in the same proportions. All r_i are also proportionate amounts and are therefore also unchanged.

Consider as an example a system in which there are three bottlenecks, through which 60%, 30% and 10% of the required supply passes. There is no redundant capacity present, and as such $X = R$ and $r_i = 1 - l_i$ with $l_1 = 0.6, l_2 = 0.9$ and $l_3 = 1$. The corresponding cumulative effects of the losses of sources 1, 2 and 3 in that order are such that the remaining supply after each loss is 40%, 10% and 0. The measure of proportionate required capacity is then $m_2 = 0.4 + 0.1 = 0.5$.

Next, we consider a second system, again with three bottlenecks, but this time with excess capacity, such that the sources produce, 70%, 45% and 20% of the total requirement. We now have $X = 1.35R$ where $r_1 = 1 - \frac{[0.7-0.35]}{1} = 0.65$, given that with a production capacity of 1.35 times the requirement, a loss of 0.70 times the requirement leaves 0.65. Following the destruction of the next source, $r_2 = 0.65 - 0.45$ or $1 - [0.7 + 0.45 - 0.35] = 0.2$. In this case, the first worst-case destructive event leaves 65% or required supply, and the loss of a second leaves 20%. The measure of proportionate required capacity is then $m_2 = 0.65 + 0.20 = 0.85$. The increase in system robustness afforded by surplus capacity in the second case system is reflect in the increased value of m_2.

We now consider the robustness of the example system structures A, A', B, C, C' and D. As demonstrated, the values of measures m_1 and m_2 will depend upon whether there is supply available beyond the requirement such that $X > R$ or not. The table below contains the values of robustness measures as defined above for cases in which $X = R$ and $X = 1.5R$.

Table 4.1: Values of measures m0, m1 and m2 for sample system structures

	$X = R$			$X = 1.5R$		
	$\mathbf{m_0}$	$\mathbf{m_1}$	$\mathbf{m_2}$	$\mathbf{m_0}$	$\mathbf{m_1}$	$\mathbf{m_2}$
A	1.39	1.39	0	1.39	2.08	0
A′	1.61	1.61	0	1.61	2.41	0
B	1.39	1.39	1.5	1.39	2.08	2.25
C	1.39	1.39	0.5	1.39	2.08	0.75
C′	1.61	1.61	0.412	1.61	2.41	0.618
D	1.39	1.39	0.5	1.39	2.08	1.125

The measure of source entropy m_0 does not reflect distinctions between cases $X = R$ and $X = 1.5R$, as values of this measure are unchanged.

The values of re-scaled entropy m_1 are higher, indicating that the extra capacity is reflected in higher robustness scores. In the cases above, the ranking of the different structures remains unchanged, since only the ratio of X and R is used, and the ability in case D to transfer output from either source to any end user is not reflected in measures 0 and 1.

The measure of proportionate required capacity does use the information, and promotes case D to a higher robustness ranking than cases C and C'. Case B remains the most highly ranked.

CHAPTER 5 APPLICATION TO ELECTRICAL INFRASTRUCTURE

We now consider an empirical application to an important element of economic infrastructure. Electricity underlies a large, if not total, portion of economic activity, and its loss can cause severe disruption and jeopardize the well-being and safety of people and industry. Alongside energy supply and water, it is among the most fundamental infrastructural element of a typical developed economy.

In an effort to compare, contrast and evaluate the two main approaches highlighted in Sections 4 and 5 above, we treat the electrical power generation and distribution networks of the four largest Canadian provinces: British Columbia (BC), Ontario (ON), Quebec (QC) and Alberta (AB). In each instance, system maps, locations and capacities of generating stations and substations are in the public domain. The most relevant portions pertaining to the evaluation of robustness can be consulted in Appendix A and associated references.

In the following chapter, we begin by studying the vulnerability of these electrical transmission networks using a network-theory based approach. We then conduct a second analysis from an entropy-based perspective, before discussing similarities, differences, strengths and limitations of the different approaches.

5.1 Network theory-based approach

The following subsection aims to present and describe the empirical networks examined in the current study, as well as the resulting graphs produced by their translation from representations in system diagrams to mathematical abstractions.

This transfer of information was completed by interpreting the various network maps and summarizing only the most relevant components into a representative adjacency matrix. In doing so, co-generation hubs, for example, which can group together many different power-generating assets, may have been grouped into a single graph component. Similarly, two separate lines spanning a same distance along the same path may have been described as one distinct edge.

Given our current research objectives, these simplifications should in no sense constrain our analysis, as our focus is on those major elements—production centers, transfer bottlenecks and delivery hubs—which most consequentially impact network dynamics.

5.1.1 British Columbia

Information pertaining to hydroelectric power generation and transmission in British Columbia was available in the public domain, via the province's independent system operator (ISO) BC Hydro, and can be consulted in Appendix A (BC Hydro, 2016).

Over 90% of energy produced in the province is by hydroelectric generation, with 80% of the effective generating capacity concentrated at hydroelectric installations in the Peace and Columbia river basins (BC Hydro, 2016). The province's transmission infrastructure is made up of 18,286 kilometers of high-voltage lines, 22,000 steel towers and 292 substations connecting the major generation hubs in the northern and southern interior regions with the major load centres in heavily populated areas of southwest B.C., where approximately 70% to 80% of the province's electrical power is consumed (BC Hydro, 2016).

Drawn as a 30-node mathematical graph, B.C's electrical transmission grid resembles the network illustrated in Figure 4 below.

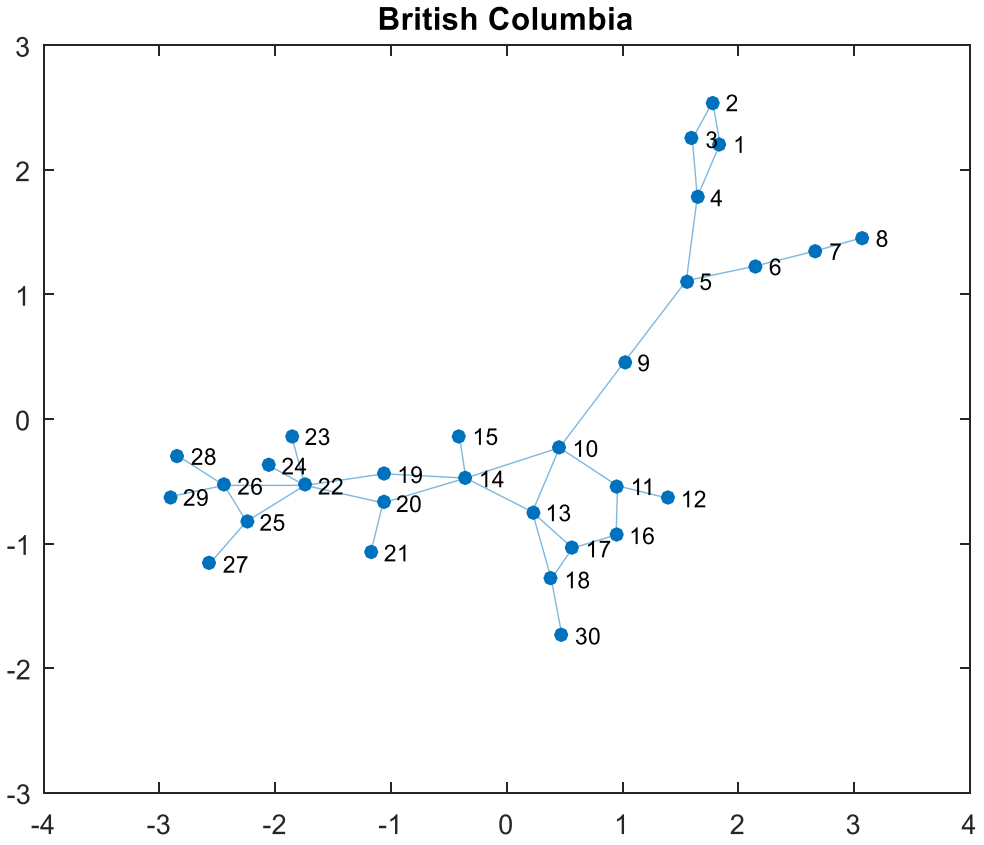


Figure 5.1: B.C. Bulk Transmission System

The nodes contained in the electrical transmission network take on different values when ranked in terms of degree, betweeness, closeness and eigenvector centrality.

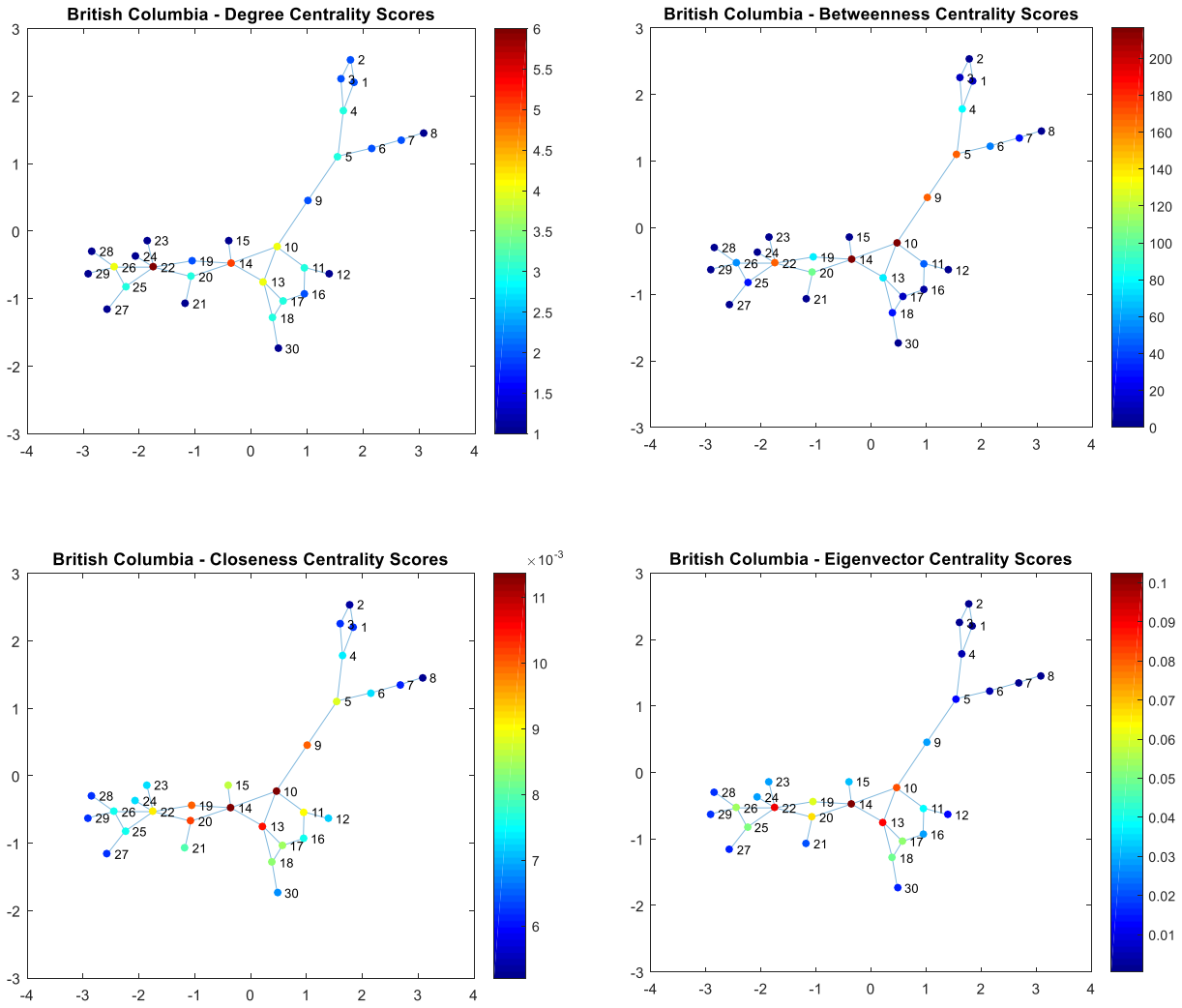


Figure 5.2: Centrality scores - B.C.'s Bulk Transmission Grid

While the figure above provides a useful overview of the variation in terms of node ranking, a detailed list of individual node centrality scores can be consulted in Appendix B.

5.1.2 Ontario

As with British Columbia, information on Ontario's electricity generation and transmission was available via the province's chief operator, IESO, and while production capacity and output

information pertaining to the province's main power generating installations is available online and updated regularly, the same cannot be said regarding the provinces electrical transmission maps, which were last updated in 2009. As such, power output values used in the subsequent study date back to 2009 (IESO, 2016a).

The province's installed generation capacity totals approximately 35,951 MW. Of this supply, 36%, 28% and 23% is generated by nuclear, gas and hydroelectric sites, respectively, which make up the province's baseline production. The remaining fraction of power is provided by intermittent renewable sources, such as wind, solar and biofuel, which supplement the production of electricity during peak periods of demand (IESO, 2016b). A system map and can be consulted in Appendix A (IESO, 2016b).

Ontario's power generation and transmission system produces the 65-node network illustrated in the figure below.

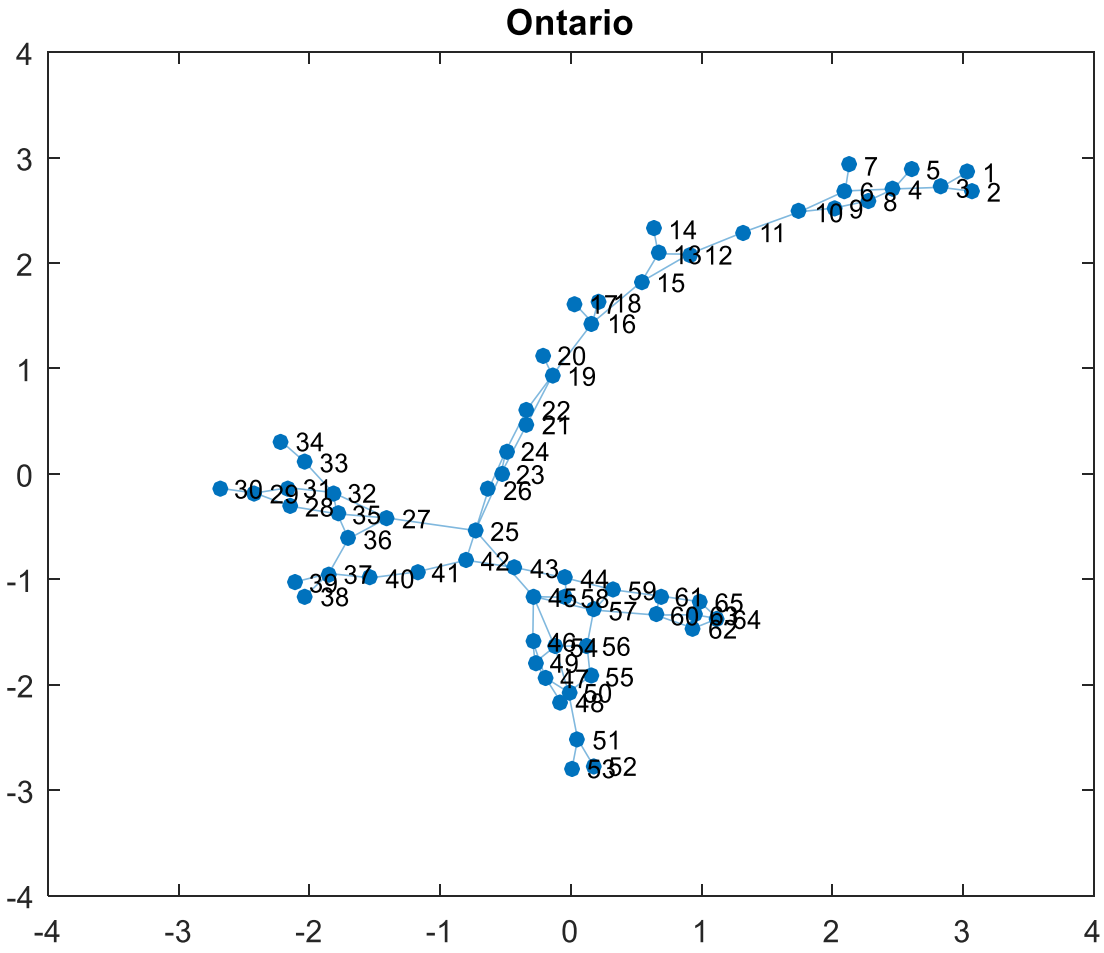


Figure 5.3: Ontario Bulk Transmission System

In ranking the nodes of the graph above according to the various centrality measures, we obtain diverging results, as highlighted by the figure below.

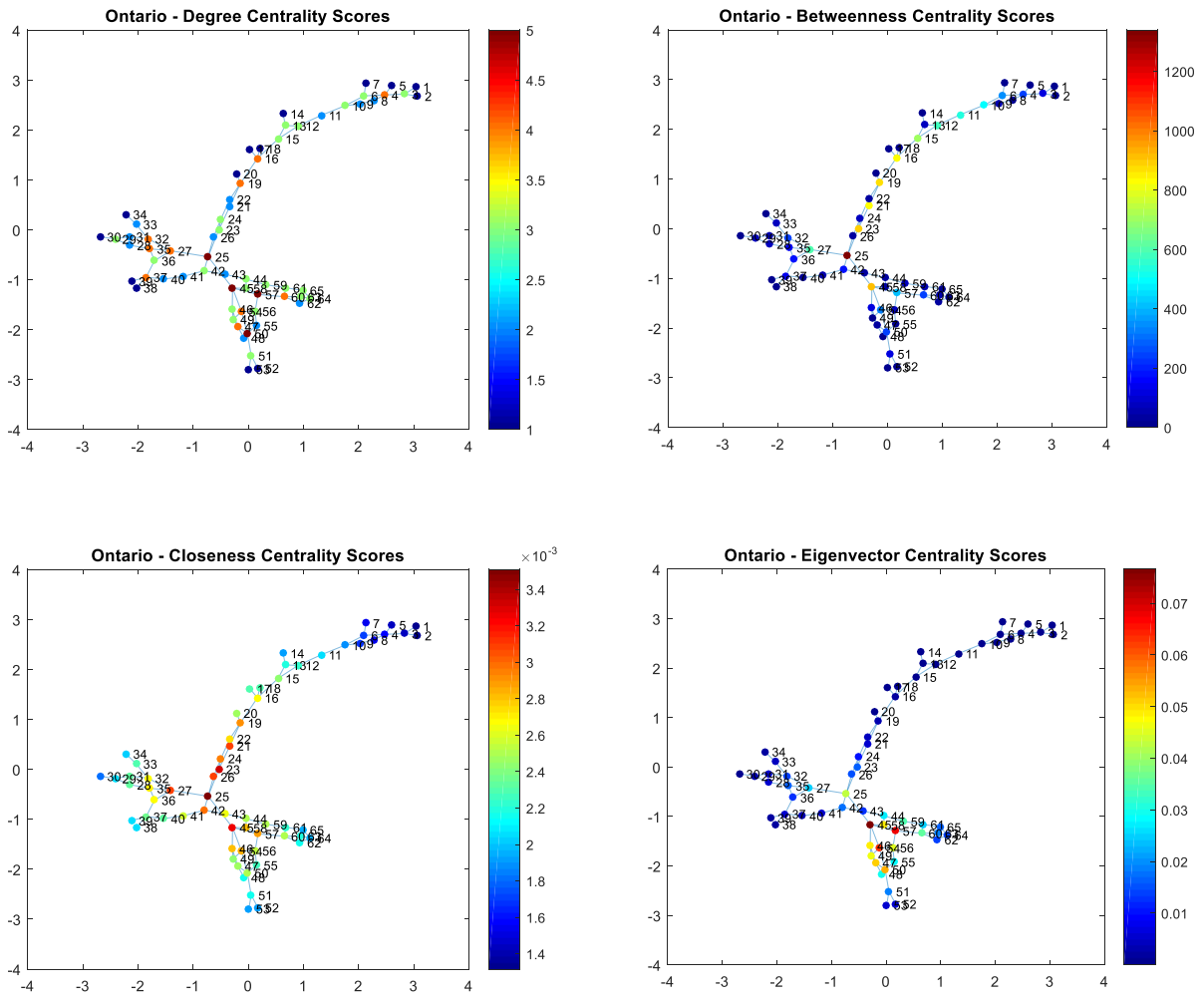


Figure 5.4: Centrality Scores - Ontario's Bulk Transmission System

The specific scores of individual nodes can be consulted in Appendix B.

5.1.3 Quebec

System maps and generation capacities for the province of Quebec were obtained via the region's operator, Hydro-Quebec. System maps have been attached in Appendix A.

As with British Columbia, Quebec's main source of power generation stems from hydroelectricity. The province's sources of production include 61 hydroelectric generating stations and one thermal generating station which represent Quebec's total installed capacity of 36,500 MW (Hydro Qc, 2016a).

The Hydro-Quebec TransEnergie transmission system is the most extensive in North America, and includes 533 substations and over 32,272 kilometers of high-voltage lines (Hydro Qc, 2016b).

Represented as a mathematical graph, Quebec's transmission network resembles the 61-node network illustrated below.

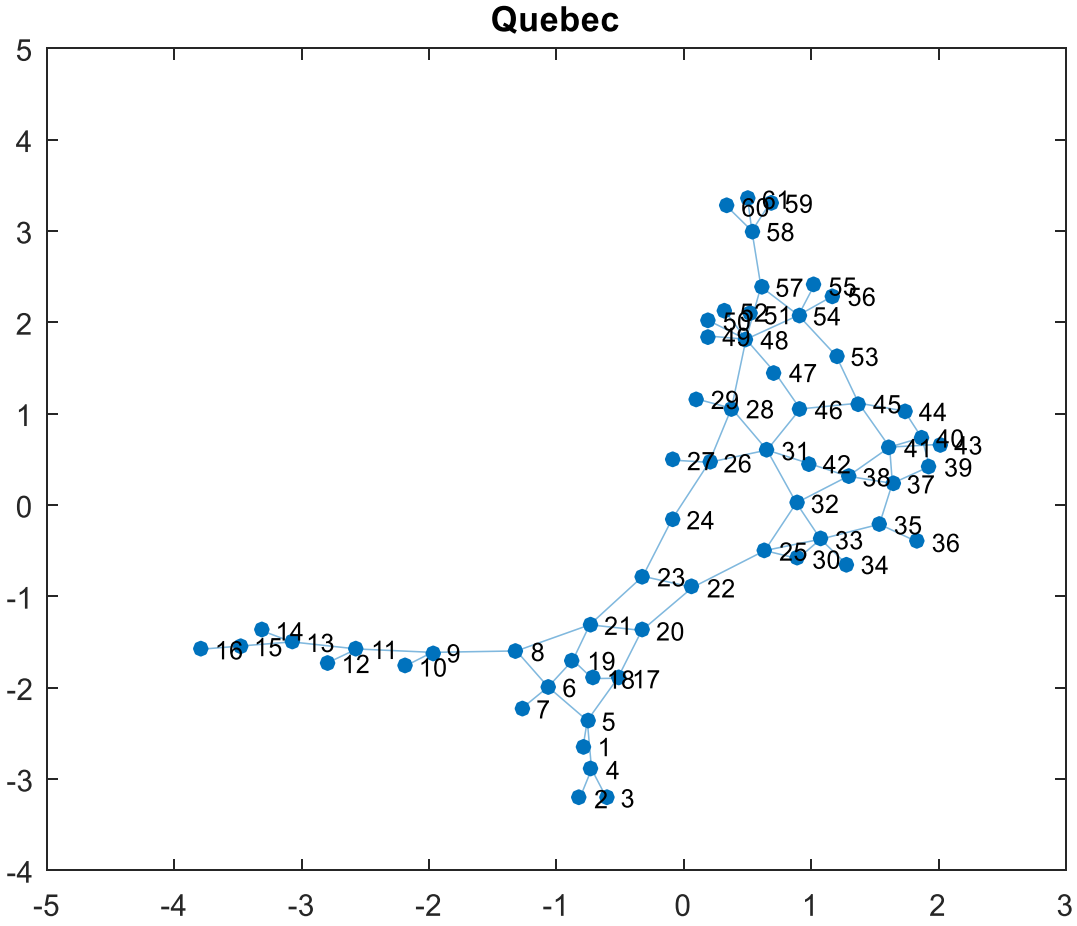


Figure 5.5: Quebec's Bulk Transmission System

As with other networks, we provide an overview of the variability of results obtained when ranking nodes in accordance with different centrality measures in the figure below. The exact values obtained can be consulted in Appendix B.

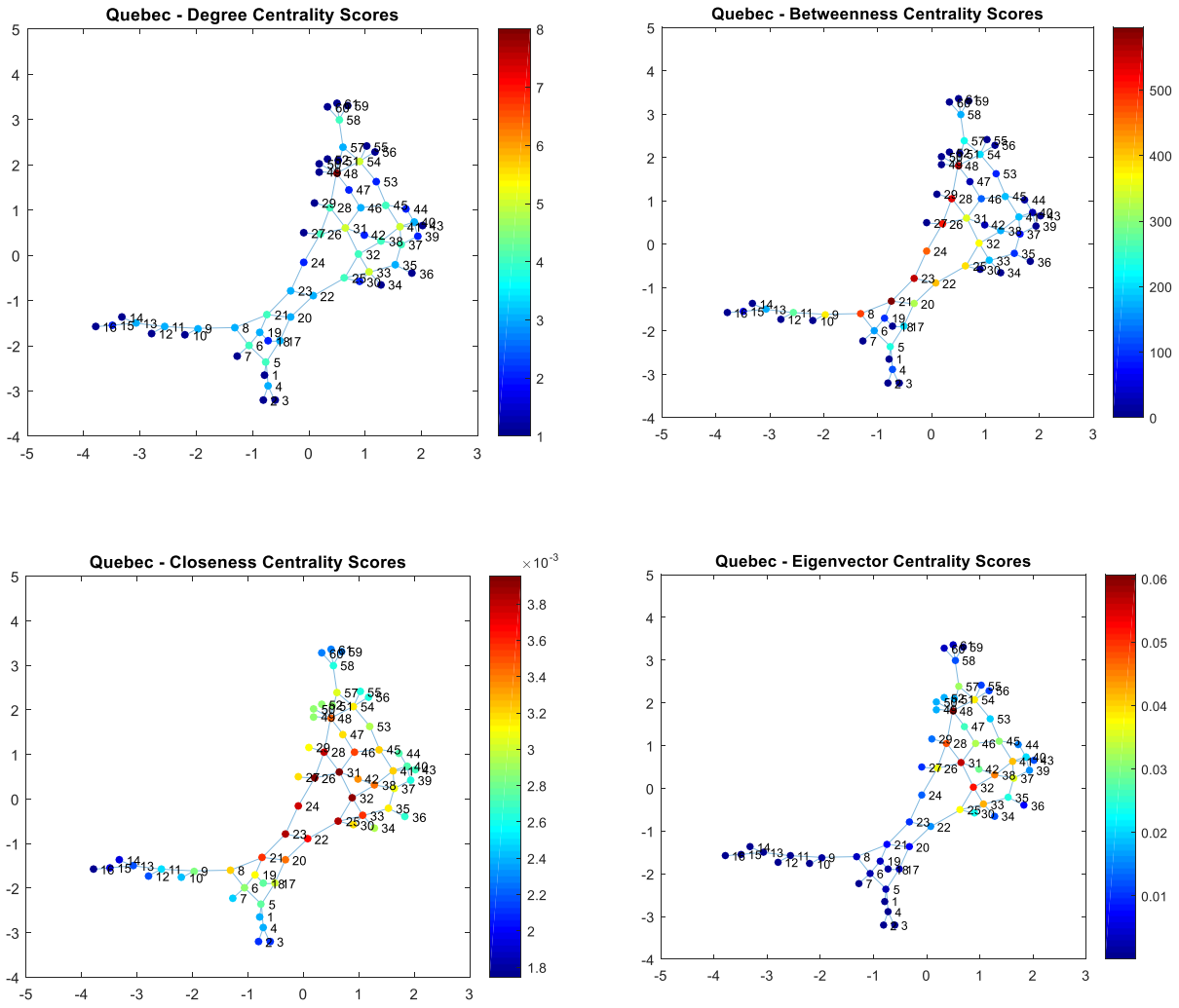


Figure 5.6: Centrality Scores – Quebec's Bulk Transmission System

5.1.4 Alberta

Lastly, information gathered on Alberta's electrical generation network was originally compiled by Alberta Energy, the province's chief energy development agency, and by AESO, the Alberta Energy System Operator.

The province's current installed generating capacity stands at 16,261 MW, the bulk of which is produced by thermal plants fueled by either coal or natural gas (Alberta, 2007). As of December 2015, 10% of the province's generation is by hydro, wind and biomass assets.

For the purpose of our research, information pertaining to Alberta's transmission grid was obtained via a study on the efficiency of Alberta's electrical supply system, prepared by Jem Energy. Relevant excerpts can be consulted in Appendix A (Jem Energy, 2004).

Modeled as a 49-node graph, Alberta's bulk transmission system resembles the network displayed in the figure below.

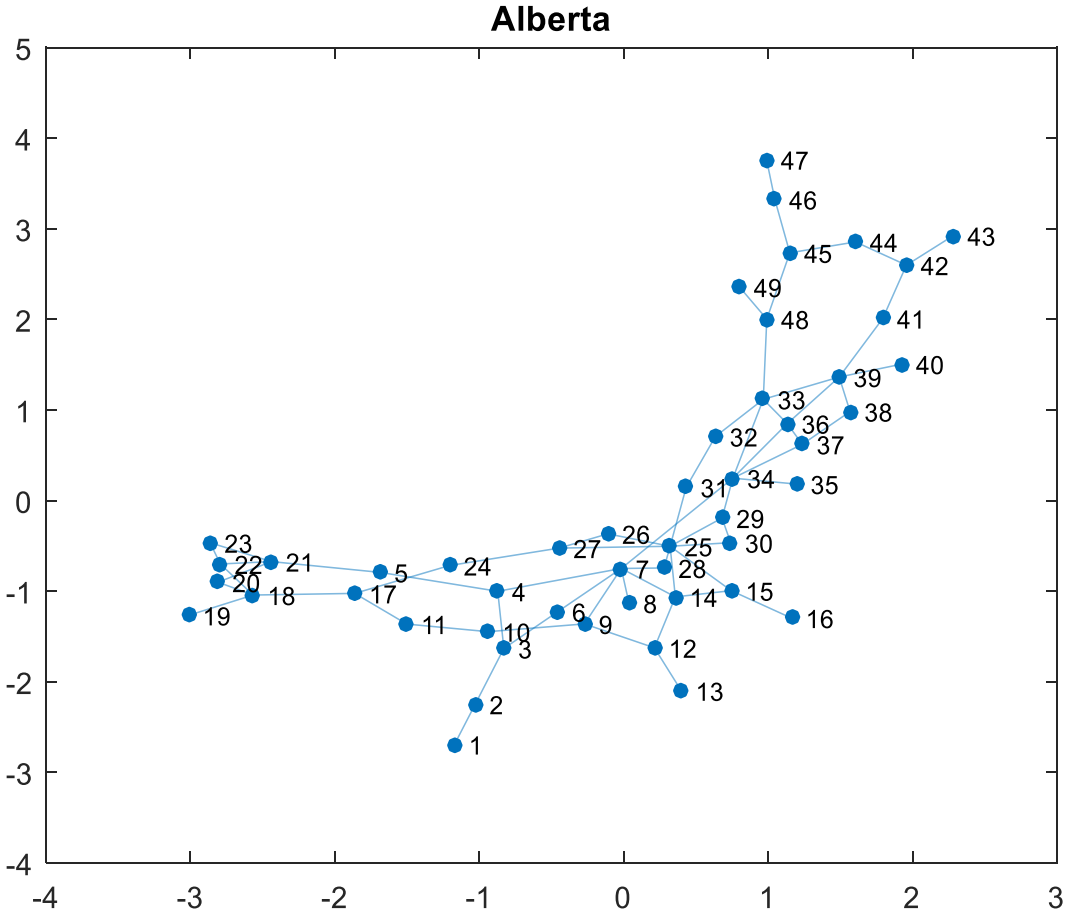


Figure 5.7: Alberta's Bulk Transmission System

Ranking the nodes above in terms of different centrality measures provides diverging results, which can be overviewed in the figure below, or consulted in Appendix B.

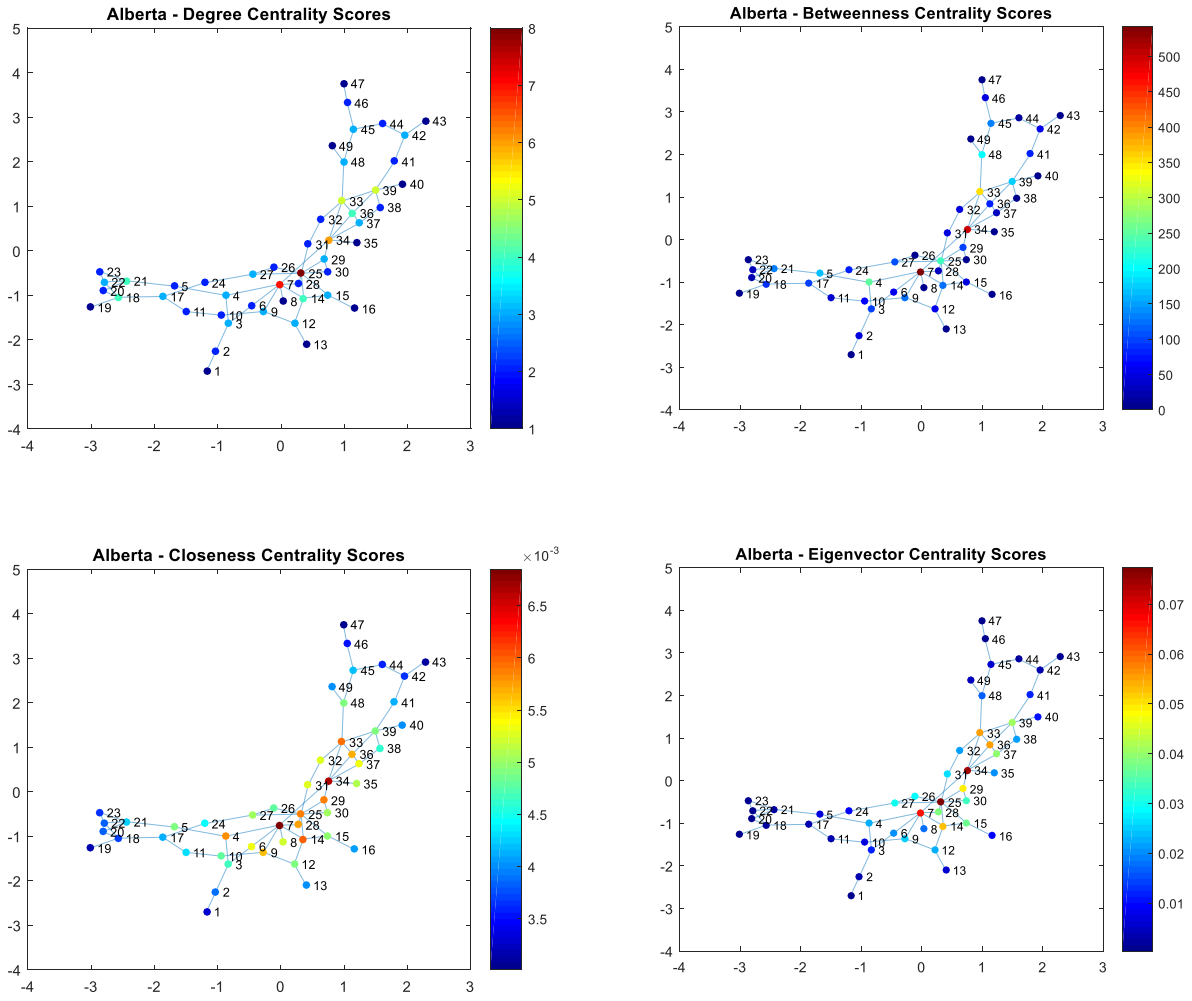


Figure 5.8: Centrality Scores - Alberta's Bulk Transmission System

5.1.5 Network Characteristics

Using the topological information contained within the adjacency matrixes of the graphs displayed above, we can calculate the basic characteristics of individual networks presented in Section 3.2. They are aggregated in the table below.

Table 5.1: Basic properties of empirical networks

	n	m	L	D	d_G	C	M	r	E_{glob}
BC	30	35	4.5609	10	2.3333	0.0455	0.1091	-0.1850	0.3128
ON	65	85	7.0611	17	2.6154	0.0419	0.1680	-0.0239	0.2190
QC	61	77	5.9077	14	2.5246	0.0286	0.1453	-0.3036	0.2441
AB	49	65	4.6565	12	2.6531	0.0467	0.1828	-0.1381	0.2890

We first note that while each of the studied real-world networks is unique, they are of similar rough orders of magnitude, ranging from 30 to 65 nodes at most. It is also clear that the order, average path length (L) and diameter (D) of the studied networks are proportionate.

The average vertex degrees range from 2.3333 to 2.6531 for British Columbia and Alberta, respectively. These results are in line with an extremely detailed study of the 4,941-node power grid of the Western United States, completed by Watts, which found an average degree of 2.6691 edges per vertex (Watts, 2016). The distribution of degrees across the multiple nodes in the networks is summarized in the figure below

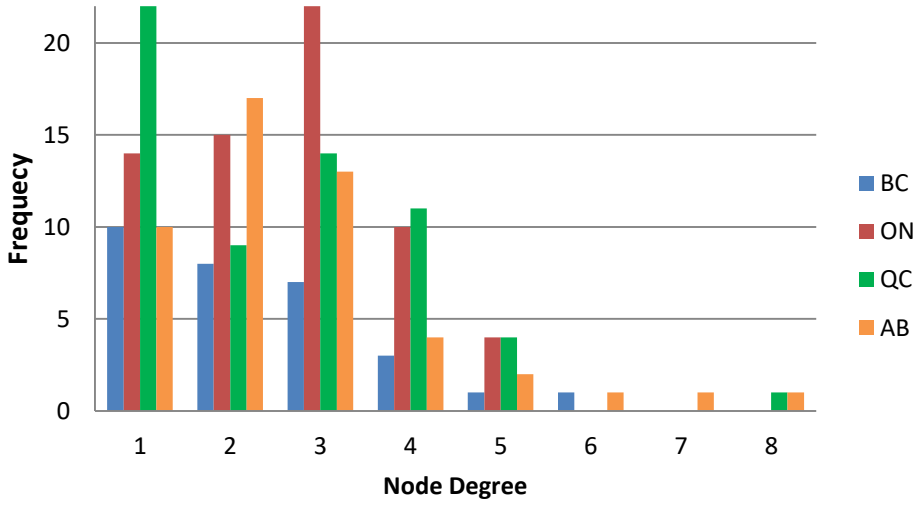


Figure 5.9: Node degree distributions

These distributions, although imperfect, resemble a Power Law trend, whereby a small fraction of a given network's nodes are highly connected, with the remaining nodes having medium to low levels of connectivity. These results are unsurprising, as past studies into the prevalence of Power Laws within economic systems have shown that the size of urban areas within the United States are consistently well described by Power Laws (Krugman, 1996). It would therefore be only natural that the infrastructures developed to support these cities demonstrate similar distributions themselves. Power Law degree distributions are a commonly observed feature of many other real-world scale-free networks (Newman, 2003) and are said to predict heightened susceptibility to targeted attacks (Albert et al., 2000).

Levels of redundancy were computed for all provinces. Each network studied displayed minimal levels of redundancy, with Quebec's clustering coefficient trailing far below those of the other provinces, at $C_{QC} = 0.0286$. In terms of meshedness, calculated values ranged from $M_{BC} = 0.1091$ to $M_{AB} = 0.1828$, which are typical values for hierarchal, tree-like networks such as utilities infrastructures.

All networks ranked as disassortative, with ratios $r < 0$. This once again reflects results published throughout the literature, which commonly display biological and technological networks as being disassortative (Newman, 2002).

Lastly, British Columbia outranked other provinces in terms of global network efficiency, with a coefficient of $E_{BC} = 0.3128$.

5.1.6 Network Analysis

In an effort to study the robustness (or vulnerability) of Canadian provinces' electrical infrastructures, connectivity loss was used as the primary measure of network functionality. In each instance, the following sequence of calculations was performed in order to obtain required values:

1. Compute degree, betweeness, closeness and eigenvector centrality scores for every node in the BC, ON, QC and AB networks;
2. For each centrality measure, rank the nodes from highest to lowest value;

3. For each province network, remove nodes (as well as their associated edges) as ordered according to the centrality measure of choice, computing the size of the largest remaining subgraph after each subsequent node is eliminated;
4. Compute connectivity loss for each node removal;
5. Plot connectivity loss as a function of the fraction of nodes removed.

Following the sequence of steps above, connectivity loss, calculated for every province, according to each centrality score, produced the results display in the figure below.

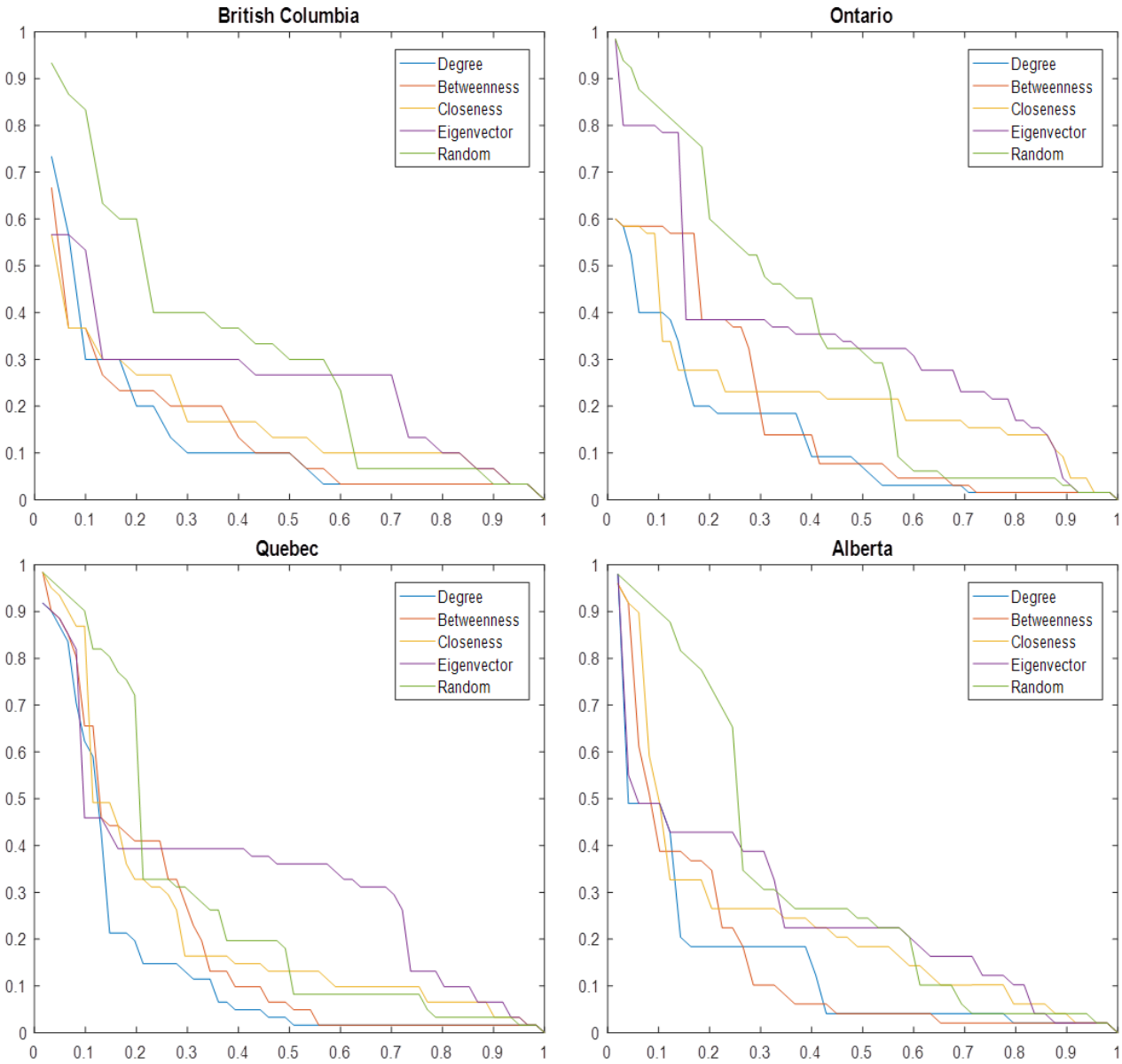


Figure 5.10: Connectivty Loss (y-axis) according to Fraction of nodes removed (x-axis)

The results displayed above provide an overview of how global connectivity (and consequently, functionality) of the different networks devolves as a function of the fraction of nodes removed in the percolation processes.

Using these results, we can compute single-value measures of graph vulnerability and robustness, as defined in Section 3.2. For each province and centrality-based preferential ranking, we obtain the following vulnerability measures.

Table 5.2: Vulnerability Scores

	V_{BC}	V_{ON}	V_{QC}	V_{AB}
Degree	0.3689	0.3703	0.3551	0.3605
Betweenness	0.3622	0.3211	0.3019	0.3517
Closeness	0.3322	0.2796	0.2705	0.2747
Eigenvector	0.2522	0.1608	0.1686	0.2518
Random	0.1922	0.1684	0.2267	0.1822

Conditional formatting of the different cells above allows us to efficiently identify which of the provinces were most vulnerable, and under what type of ordered attack.

For each network, node removal in terms of degree centrality proved to be the most effective means of degrading network functionality, with only minimal variation in vulnerability scores across all four provinces. Ranking vertices in terms of highest degree in this instance seemingly followed a Pareto rule, whereby the removal of only 15% to 20% of nodes achieved an 80% reduction in global network connectivity.

Betweeness centrality and closeness centrality were the second and third most effective node removal schemes, respectively, when examining both *V*-scores and graphical results. Removing nodes in terms of eigenvector centrality proved to be much less effective at degrading network performance, rivaling and at times underperforming the effectiveness of random node selection.

Perhaps most interestingly, however, is that for each province, with exception to Ontario, the first 10% of nodes removed resulted in similar initial drops in global connectivity regardless of the chosen centrality measure.

Initial interpretation of the results above would suggest that despite being a rather simple measure of node importance, degree centrality—and hence, node connectivity—provides a sufficient level of information when aiming to degrade network functionality. This is unsurprising, though, given that the underlying assumption of the current study is that connectivity loss is the most insightful measure of a network's performance or survivability.

5.2 Entropy-based approach

The following section presents the results of the entropy-based infrastructure robustness methodologies when applied to the major Canadian electrical grids presented above.

Again, we note that we distinguish the robustness calculation from that of the reliability calculation—more common in engineering applications—which estimates the probability of continued adequate functioning of a system for a specified period of time. Here, the proposed measures do not estimate likelihood of proper functioning, but rather the consequences associated with a sequence of catastrophic events.

Information on the capacities and outputs of electrical production sites in the cases of British Columbia, Ontario, Quebec and Alberta were available in the public domain, and can be consulted in Appendix A. Given this information, we are able to calculate measures m_0, m_1 and m_2. Of course, complex engineering systems on the whole, and electrical power infrastructures in specific, are in a constant state of flux as changes in supply come into effect in order to perfectly match varying demand profiles. Similarly, system configurations are also subject to change as new capacity is added and older stations are removed from service or decommissioned entirely. The results presented herein are therefore a snapshot of a particular point in time.

The figure below provides a graphical representation of some of the raw data obtained via the different independent system operators in the form of a cumulative distribution function (CDF) of the sources of supply (electrical generation sites) of the four grids under study. The outputs of sources are divided by total supply to produce proportionate sources.

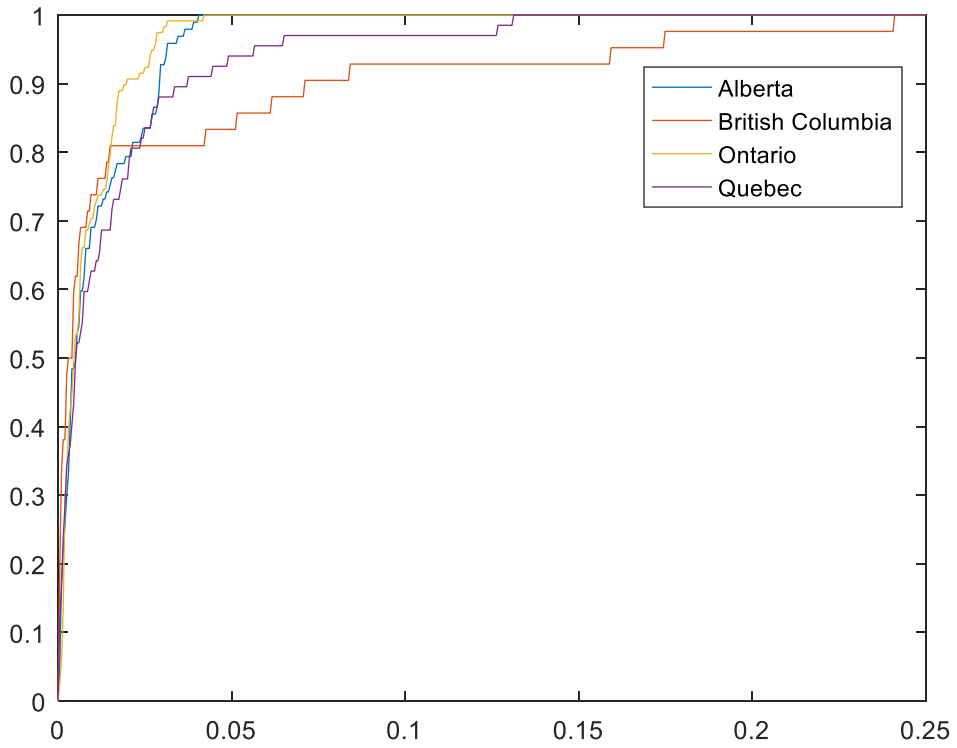


Figure 5.11: CDFs of proportionate sources of supply (xi/X) of Canadian power grids

Proportionately large sources produce the right-hand elements of the CDFs, and as such, we expect systems with relatively long right-hand parts to have relatively low robustness.

Information in the plot above does not, however, produce results providing insight on a given system's most vulnerable points, such as bottlenecks. This information is captured by measure m_2.

The figure below illustrates proportions of remaining requirement r_i for a sequence of i maximally destructive events where $i = 1, 2, \ldots, 12$. The resulting graph is a form of survivor function, where higher lines are indicative of relative robustness. It also ranks the different provinces in order of robustness, which we would expect to see reflected in m_2.

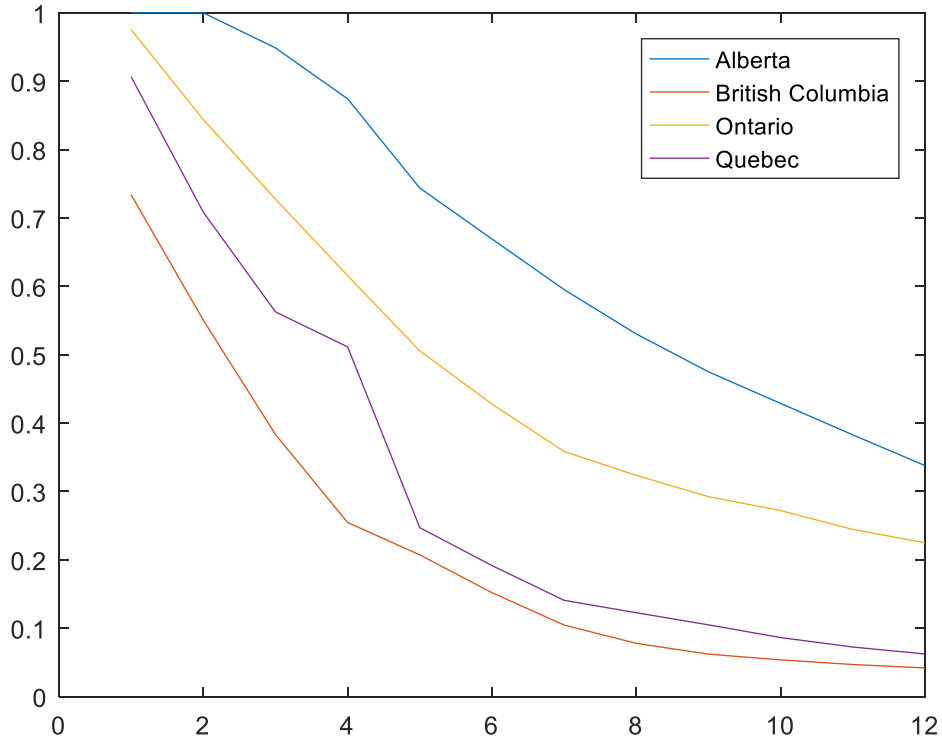


Figure 5.12: ri vs. i (Survivor functions) of Canadian power grids

We now consider numerical values for the infrastructures of the four Canadian provinces. Given the necessary input requirements, computing values for m_0 and m_1 is straightforward, whereas m_2 requires careful examination of system structure in order to understand losses incurred conditional on n destructive events occurring.

To produce values of proportionate required supply r_i remaining following such events, we begin by identifying the single largest bottleneck A which, if destroyed, would result in the single largest loss of electricity to consumers. We then identify the two bottlenecks which, if destroyed, would result in the greatest joint loss of supply, and so on. We note that this does not necessarily imply selected the second largest bottleneck and using it in combination with the first. In practice, it may be that two bottlenecks B and C together may produce a greater loss than A with any one other.

For example, we consider a case in which the loss of the single largest source results in a loss of z. It may be possible that two other sources, each connected to consumers by two distinct routes, exist such that neither can be removed from the supply system via a single destructive event.

However, we can imagine that if both routes are removed by the elimination of two separate bottlenecks, the resulting loss is e.g. $2.5z$.

The following table contains measures m_0, m_1 and m_2 for the selected Canadian provinces.

Table 5.3: Measures m0, m1 and m2 for Canadian power grids

	m_0	m_1	m_2
BC	2.39	2.51	2.88
ON	4.15	4.78	8.72
QC	3.35	3.86	4.28
AB	3.90	4.56	16.08

The results show clear distinctions between the robustness values of different systems. When grading systems according to entropy measures m_0 and m_1, Ontario ranks as the most robust province, and Alberta as the runner-up. When grading in terms of m_2, however, Alberta far outperforms the other Canadian provinces, with Ontario's electrical system ranking second. As with the generic example discussed in subsection 4.1.2.3 above, the excess capacity taken into account in measure m_1 is reflected in the higher robustness score.

By ordering systems according to m_2, we obtain the same ranking as displayed in the graph above, as expected.

5.3 Discussion

Prior to attempting a comparative analysis between the two CI vulnerability approaches presented above, it is important to highlight the unique characteristics and inherent differences between models.

Network-based approaches study the robustness of systems to a variety of different sequential attack schemes, based on topological measures. In the case study presented above, for which only high-level open-source information was available, the vulnerability analysis focused solely on topological aspects of the different power grids, and while certain centrality measures can be used to provide insights on flow patterns, it remained a study on the connectivity of networks.

The entropy-based analysis also focused on topological features, but sought to highlight the supply and demand requirements of the grids under study. Nodes for percolation were selected in

accordance with maximal loss of supply for a number of destructive events, resulting in a model which captures the flow-based intricacies of a given network.

Unsurprisingly, the different approaches produced diverging results, as displayed in the table below.

Table 5.4: Canadian provinces, from most to least vulnerable

	Degree	***Betweenness***	***Closeness***	***Eigenvector***	m_0	m_1	m_2
1	ON	BC	BC	BC	BC	BC	BC
2	BC	AB	ON	AB	QC	QC	QC
3	AB	ON	AB	QC	ON	AB	AB
4	QC	QC	QC	ON	AB	ON	ON

In the case of the network theory-based model—using degree centrality as a measure of node ordering—the Canadian provinces were ranked, from most to least vulnerable, as follows: ON, BC, AB and QC. For the entropy-based approach, the provinces were ranked as BC, QC, ON and AB from most to least vulnerable using m_2, and BC, QC, AB and ON for both m_0 and m_1.

In comparing the two methodologies, the only apparent consistency is in the ranking of British Columbia as the most vulnerable province. Empirically, BC ranked lower than other provinces in terms of meshedness, implying that lower levels of redundancy may account for the network's rapid deterioration. Similarly, the western province outpaced the other systems in terms of global efficiency—a measure of parallel system efficiency—which may in fact provide insights as to the propagation of errors. This finding echoes the hypothesis presented as part of this paper's introduction, suggesting that a trade-off exists between CI system efficiency and vulnerability.

The economic significance of the disparities between provinces, however, is difficult to ascertain. Certain measures fail to reflect loss of output, making direct vulnerability comparisons and cost estimates associated to infrastructure improvements challenging.

Fundamentally, the two distinct approaches to the assessment of network vulnerability prioritized different elements of robustness, either topology or flow, and as such, failed to provide similar insights into overall CI system vulnerability.

CHAPTER 6 CONCLUSION AND RECOMMENDATIONS

Critical infrastructure systems are the physical assets that provide modern societies with the fundamental resources required to conduct essential economic and social operations, from power and electricity to drinking water and telecommunications. The crucial importance of these vast, complex and ubiquitous infrastructures is widely acknowledged and as such, the necessity to protect these networks from destructive events—both intentional and accidental—has garnered the attention of researchers and security experts alike. Similarly, it is also well recognized that the cost and effort associated with total protection presents an enormous challenge. Society will achieve its greatest return on investment by correctly identifying, prioritizing and protecting the most vulnerable assets in its infrastructure portfolio. This implies the need for a screening methodology by which we can target the most crucial assets, and effective metrics with which to gauge the vulnerability of a given network as a whole, allowing us to assess risk levels and evaluate proposed or completed engineering changes.

There is considerable divergence, however, on the different approaches by which we go about doing so. Reliability engineers, for example, adopt a probabilistic approach and attempt to identify the components which are most likely to fail, assessing vulnerability as an aggregate of these probabilistic measures. Resilience-based approaches focus instead on measuring a system's vulnerability according to the time delay from the disruption event to the return to normal operations.

Robustness-based approaches measure a system's vulnerability based on its ability to maintain adequate levels of service once one or more of its components has been degraded. In the case of CI systems, that which we are most interested in is an infrastructure's ability to meet its demand requirements conditional on some disruptive event having taken place. Factors which will determine a network's robustness are certain topological features, such as the presence of bottlenecks, redundant features and the location of production sites, as well as its supply and demand dynamics, including excess production capacity.

The present study compared the relative value of diverging approaches to CI network vulnerability assessment: network theory-based and entropy-based models. Our interest in studying the individual models was to assess if they tended towards similar conclusions, despite valuing different aspects of system robustness. In order to do so, an empirical application of both

models was carried out on the electrical transmission networks of the four largest Canadian provinces, using information available in the public domain.

Network-based models valued the connectivity of systems above all, while the entropy-based approach considered the total remaining supply following some destructive event, with each model requiring different input data and calculations.

Network characterization and analysis subsections provided results consistent with values contained in the associated literature, validating the modeling of transmission grids from system diagrams to mathematical graphs.

Our attempt to investigate the similarities between the separate methodologies failed to provide any meaningful consistencies when comparing provinces' robustness according to the different grading schemes. Network measures produced rankings of provinces which differed greatly from what is observed in the loss of capacity diagrams. To the extent that one is interested in the potential for targeted attacks to remove capacity, these measures may provide unreliable indicators. Policymakers interested in robustness to targeted attacks may wish to work with a variety of the measures. For instance, network performance measures and remaining proportionate supply metrics provide policy experts and security analysts with global vulnerability measures, enabling them to assess the need for additional protection, while centrality measures and greatest loss sites allow them to prioritize efforts and evaluate potential engineering changes.

As a final note, it is important to highlight that while the research and findings above offer some valuable insights and promising methodologies, they are presented here in their first iteration and as such, reflect only modest levels of maturity. As discussed below, future refinement and calibration efforts—enabled by access to more detailed operational data and expert opinion—will allow for higher fidelity modeling and more reliable and conclusive insights.

6.1 Future research

Lastly, no work of scientific research is complete without a discussion on potential improvements and opportunities for future research. Below, we highlight possibilities for the improvement of the entropy-based model, presented here in its first iteration, and present options for its future development. Unsurprisingly, many of these improvements are interrelated.

6.1.1 Improvement

6.1.1.1 Data

With all economic, engineering and scientific modeling, the ability to accurately and precisely simulate the outcome of a phenomenon rests on two variables: the validity of the model at hand and the quality of the input data.

As was underscored in previous sections, the majority of critical infrastructure assets are owned and operated by private interests and as such, access to detailed operational data is limited. While information available and collected via the public domain may have been sufficient in establishing a first proof of concept, as presented in Chapters 4 and 5, access to detailed operational data would prove useful in future refinement and calibration efforts.

As such, a first recommendation is to encourage the establishment of research partnerships with relevant CI system owners and operators. Furthermore, despite our current interest in electrical transmission networks, we recognize the need to extend this research beyond the power and utilities sector, and validate the proposed model's ability to capture the robustness of other critical networks. Potential candidates for future empirical analysis include oil and gas pipelines, global shipping routes, telecommunications networks, international and regional flight paths and other industrial supply chains.

6.1.2 Future development

Following a valid first proof of concept, there exist several avenues for the future development of the entropy-based model. Among the most promising and useful developments under consideration are the addition of directed and weighted elements, the automation of supply calculations, the consideration of storage capabilities and the representation of interdependent heterogeneous networks.

6.1.2.1 Directed and weighted graphs

As mentioned in Chapter 2, directed and weighted graphs allow for more detailed modeling of networked processes. In the case of CI systems, directed and weighted edges can model the direction in which flow travels and the quantities of resources being transited, respectively. Provided that more detailed operational data can be obtained, updating the adjacency matrices of

the graphs above and others like it would prove useful in that it would provide a more complete understanding of a given system, and facilitate the calculation of the entropy-based measures.

6.1.2.2 Automated calculus

A considerable limitation of the current model is its inability to be automated simply, given that the proportionate remaining supply calculations can vary between systems. The addition of directed and weighted edges proposed above would result in a blended network-and-entropy model, and provide the capability of using common mathematical programming tools, such as MATLAB, in order to automate the calculation of relevant values, i.e. node in-degree and out-degree and node in-flow and out-flow. Achieving this would constitute a major improvement, facilitating the analysis of larger, more detailed networks.

6.1.2.3 Storage capabilities

While the proposed model was designed in order to account for the robustness gains achieved by excess production capacity, it fails to capture the reduction in vulnerability that can be attained thanks to storage capacities present within a given system. In the case of electrical transmission networks, for which only modest amounts of storage can be achieved, the ability to reflect reserves would display minimal changes to overall robustness. In other networks, such as oil and gas supply chains, excess storage and strategic reserves—distinct from excess production and supply—are key elements of thoughtful engineering design, and should be incorporated into the entropy-based model's key properties and measures.

6.1.2.4 Interdependencies

Lastly, a growing body of CI protection work is concerned with the study of interdependent systems. Rarely do real-world systems operate in isolation. More often than not, critical infrastructures are intertwined, with output from one sector becoming the input to another, giving rise to the possibility of cascading failures in the event of a component failure. In fact, research into mixed and interdependent networks has shown that coupled networks behave differently than their individual counterparts (Buldyrev, Parshani, Paul, Stanley, & Havlin, 2010). One example of this phenomenon is the natural gas-fueled production of electricity in the United States, where gas networks rely on electricity and electrical networks rely on energy supply. Future developments of the proposed model should attempt to capture these interdependency risks.

BIBLIOGRAPHY

Albert, null, Jeong, null, & Barabasi, null. (2000). Error and attack tolerance of complex networks. *Nature*, *406*(6794), 378–382. https://doi.org/10.1038/35019019

Albert, R., Albert, I., & Nakarado, G. L. (2004). Structural vulnerability of the North American power grid. *Physical Review E*, *69*(2), 25103. https://doi.org/10.1103/PhysRevE.69.025103

Albert, R., & Barabási, A.-L. (2002). Statistical mechanics of complex networks. *Reviews of Modern Physics*, *74*(1), 47–97. https://doi.org/10.1103/RevModPhys.74.47

Alberta, G. of. (2007, June 19). Electricity Statistics [Text]. Retrieved August 28, 2016, from http://www.energy.alberta.ca/electricity/682.asp

Anderson, C. W., Santos, J. R., & Haimes, Y. Y. (2007). A Risk-based Input–Output Methodology for Measuring the Effects of the August 2003 Northeast Blackout. *Economic Systems Research*, *19*(2), 183–204. https://doi.org/10.1080/09535310701330233

Attoh-Okine, N. O., Cooper, A. T., & Mensah, S. A. (2009). Formulation of Resilience Index of Urban Infrastructure Using Belief Functions. *IEEE Systems Journal*, *3*(2), 147–153. https://doi.org/10.1109/JSYST.2009.2019148

Ayyub, B. M. (2014). Systems resilience for multihazard environments: definition, metrics, and valuation for decision making. *Risk Analysis: An Official Publication of the Society for Risk Analysis*, *34*(2), 340–355. https://doi.org/10.1111/risa.12093

Barabási, A.-L. (2003). Scale-Free Networks. Retrieved November 14, 2016, from https://www.scientificamerican.com/article/scale-free-networks/

Barabási, A.-L., & Albert, R. (1999). Emergence of Scaling in Random Networks. *Science*, *286*(5439), 509–512. https://doi.org/10.1126/science.286.5439.509

Barrat, A., & Weigt, M. (1999). On the properties of small-world network models. *arXiv:cond-mat/9903411*. Retrieved from http://arxiv.org/abs/cond-mat/9903411

Barton, D. C., Eidson, E. D., Schoenwald, D. A., Stamber, K. L., & Reinert, R. (2000). *Aspen-EE: An Agent-Based Model of Infrastructure Interdependency*. Sandia National Labs., Albuquerque, NM (US); Sandia National Labs., Livermore, CA (US). Retrieved from http://www.osti.gov/scitech/biblio/774027

Basu, N., Pryor, R., & Quint, T. (1998). ASPEN: A microsimulation model of the economy. *Computational Economics*, *12*(3), 223–241.

BC Hydro. (2016). BC Hydro's System. Retrieved August 28, 2016, from https://www.bchydro.com/energy-in-bc/our_system.html

BC Hydro. (2016). Maps. Retrieved November 29, 2016, from https://www.bchydro.com/energy-in-bc/our_system/transmission/transmission-system/maps.html

BC Hydro. (2016). Transmission. Retrieved August 28, 2016, from https://www.bchydro.com/energy-in-bc/our_system/transmission.html

Bonacich, P. (1972). Technique for analyzing overlapping memberships. *Sociological Methodology*, *4*, 176–185.

Borgatti, S. P. (2005). Centrality and network flow. *Social Networks*, *27*(1), 55–71.

Brown, G. G., Carlyle, W. M., Salmerón, J., & Wood, K. (2005). Analyzing the Vulnerability of Critical Infrastructure to Attack and Planning Defenses. In *Emerging Theory, Methods,*

and Applications (Vols. 1–0, pp. 102–123). INFORMS. Retrieved from http://pubsonline.informs.org/doi/abs/10.1287/educ.1053.0018

Buhl, J., Gautrais, J., Reeves, N., Solé, R. V., Valverde, S., Kuntz, P., & Theraulaz, G. (2006). Topological patterns in street networks of self-organized urban settlements. *The European Physical Journal B - Condensed Matter and Complex Systems*, *49*(4), 513–522. https://doi.org/10.1140/epjb/e2006-00085-1

Buldyrev, S. V., Parshani, R., Paul, G., Stanley, H. E., & Havlin, S. (2010). Catastrophic cascade of failures in interdependent networks. *Nature*, *464*(7291), 1025–1028. https://doi.org/10.1038/nature08932

Bush, B., Dauelsberg, L., Leclaire, R., Powell, D., Deland, S., & Samsa, M. (2005). *3 Critical Infrastructure Protection Decision Support System (CIP/DSS) Project Overview*.

Carlson, J. L., Haffenden, R. A., Bassett, G. W., Buehring, W. A., Collins, M. J., Iii, Folga, S. M., … Whitfield, R. G. (2012). *Resilience: Theory and Application.* (No. ANL/DIS-12-1, 1044521). Retrieved from http://www.osti.gov/servlets/purl/1044521/

Carrington, P. J., Scott, J., & Wasserman, S. (2005). *Models and methods in social network analysis* (Vol. 28). Cambridge university press. Retrieved from https://books.google.ca/books?hl=en&lr=&id=4Ty5xP_KcpAC&oi=fnd&pg=PR9&dq=wasserman+faust+2000+network+analysis&ots=9MJIw8x8C5&sig=mRFsA3OIni5CjFa6mNxPO5t_XMg

Cohen, null, Erez, null, ben-Avraham, null, & Havlin, null. (2000). Resilience of the internet to random breakdowns. *Physical Review Letters*, *85*(21), 4626–4628. https://doi.org/10.1103/PhysRevLett.85.4626

Cohen, R., Erez, K., ben-Avraham, D., & Havlin, S. (2001). Breakdown of the internet under intentional attack. *Physical Review Letters*, *86*(16), 3682–3685. https://doi.org/10.1103/PhysRevLett.86.3682

Cox, R. G., Barton, D. C., Reinert, R. K., Eidson, E. D., & Schoenwald, D. A. (2004). *Simulating economic effects of disruptions in the telecommunications infrastructure.* Sandia National Laboratories. Retrieved from http://www.osti.gov/scitech/biblio/918354

Crowther, K. G., & Haimes, Y. Y. (2010). Development of the multiregional inoperability input-output model (MRIIM) for spatial explicitness in preparedness of interdependent regions. *Systems Engineering*, *13*(1), 28–46. https://doi.org/10.1002/sys.20130

Department of Homeland Security. (2003). *National Strategy for Physical Protection of Critical Infrastructure and Key Assets | Homeland Security*. Retrieved from https://www.dhs.gov/national-strategy-physical-protection-critical-infrastructure-and-key-assets

Dijkstra, E. W. (1959). A Note on Two Problems in Connexion with Graphs. *NUMERISCHE MATHEMATIK*, *1*(1), 269–271.

Dudenhoeffer, D. D., Permann, M. R., & Manic, M. (2006). CIMS: A Framework for Infrastructure Interdependency Modeling and Analysis. In *Proceedings of the 2006 Winter Simulation Conference* (pp. 478–485). https://doi.org/10.1109/WSC.2006.323119

Dueñas-Osorio, L. A. (2005). *Interdependent response of networked systems to natural hazards and intentional disruptions*. Citeseer. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.330.9826&rep=rep1&type=pdf

Eidson, E. D., & Ehlen, M. A. (n.d.). NISAC Agent-Based Laboratory for Economics (N-ABLE™): Overview of Agent and Simulation Architectures. Retrieved from http://www.sandia.gov/nisac/wp/wp-content/uploads/downloads/2012/03/N-Able-Overview-of-Agent-and-Simulation-Architectures-2005-0263.pdf

Erdös, P., & Rényi, A. (1959). On random graphs, I. *Publicationes Mathematicae (Debrecen), 6*, 290–297.

Executive Office of the President. Critical Infrastructure Protection (1996). Retrieved from https://www.federalregister.gov/documents/1996/07/17/96-18351/critical-infrastructure-protection

Forrester, J. W. (1971). Counterintuitive behavior of social systems. *Theory and Decision, 2*(2), 109–140. https://doi.org/10.1007/BF00148991

Galbraith, J. W. (2009). *The Robustness of Economic Activity to Destructive Events* (SSRN Scholarly Paper No. ID 1504077). Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=1504077

Gaury, E. G. A., & Kleijnen, J. P. C. (1998). *Risk Analysis Of Robust System Design*. Retrieved from https://www.researchgate.net/publication/234756378_Risk_Analysis_Of_Robust_System_Design

Gell-Mann, M. (1994). Complex adaptive systems. Retrieved from http://authors.library.caltech.edu/60491/

Ghahramani, Z. (2006). Information Theory. In *Encyclopedia of Cognitive Science*. John Wiley & Sons, Ltd. Retrieved from http://onlinelibrary.wiley.com/doi/10.1002/0470018860.s00643/abstract

Gilbert, E. N. (1959). Random Graphs. *The Annals of Mathematical Statistics*, *30*(4), 1141–1144. https://doi.org/10.1214/aoms/1177706098

Giroux, J. (2013). Research Note on the Energy Infrastructure Attack Database (EIAD) Perspectives on Terrorism. Retrieved September 4, 2016, from http://www.terrorismanalysts.com/pt/index.php/pot/article/view/315/html

Goulter, I. C. (1987). Current and future use of systems analysis in water distribution network design. *Civil Engineering Systems*, *4*(4), 175–184. https://doi.org/10.1080/02630258708970484

Haimes, Y. Y., & Jiang, P. (2001). Leontief-Based Model of Risk in Complex Interconnected Infrastructures. *Journal of Infrastructure Systems*, *7*(1), 1–12. https://doi.org/10.1061/(ASCE)1076-0342(2001)7:1(1)

Hydro Qc. (2016a). Profile | Hydro-Québec Production. Retrieved August 28, 2016, from http://www.hydroquebec.com/generation/profil.html

Hydro Qc. (2016b). TransÉnergie | Hydro-Québec. Retrieved August 28, 2016, from http://www.hydroquebec.com/transenergie/en/reseau-bref.html

IESO. (2016a). Generator Output and Capability Report. Retrieved August 28, 2016, from http://reports.ieso.ca/public/GenOutputCapability/PUB_GenOutputCapability.xml

IESO. (2016b). IESO Supply Overview. Retrieved August 28, 2016, from http://www.ieso.ca/Pages/Power-Data/Supply.aspx

Iyer, S., Killingback, T., Sundaram, B., & Wang, Z. (2013). Attack robustness and centrality of complex networks. *PloS One*, *8*(4), e59613.

Jem Energy. (2004). A Study on the Efficiency of Alberta's Electrical Supply System. Retrieved November 29, 2016, from http://www.do-cu-cu.com/view/9b088a973da69ff452980b82a3cdd661/A-Study-on-the-Efficiency-of-Howell-Mayhew.pdf

Kaegi, M., Mock, R., & Kröger, W. (2009). Analyzing maintenance strategies by agent-based simulations: A feasibility study. *Reliability Engineering & System Safety*, *94*(9), 1416–1421.

Karnouskos, S. (2011). Stuxnet worm impact on industrial cyber-physical system security. In *IECON 2011 - 37th Annual Conference on IEEE Industrial Electronics Society* (pp. 4490–4494). https://doi.org/10.1109/IECON.2011.6120048

Kelic, A., Warren, D. E., & Phillips, L. R. (n.d.). Cyber and Physical Infrastructure Interdependencies. Retrieved from http://prod.sandia.gov/techlib/access-control.cgi/2008/086192.pdf

Krugman, P. (1996). Confronting the Mystery of Urban Hierarchy. *Journal of the Japanese and International Economies*, *10*(4), 399–418. https://doi.org/10.1006/jjie.1996.0023

Latora, V., & Marchiori, M. (2001). Efficient Behavior of Small-World Networks. *Physical Review Letters*, *87*(19), 198701. https://doi.org/10.1103/PhysRevLett.87.198701

Leontief, W. (Ed.). (1986). *Input-Output Economics* (2 edition). New York: Oxford University Press.

Lewis, T. G. (2006). *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*. John Wiley & Sons.

Lian, C., & Haimes, Y. Y. (2006). Managing the risk of terrorism to interdependent infrastructure systems through the dynamic inoperability input–output model. *Systems Engineering*, *9*(3), 241–258. https://doi.org/10.1002/sys.20051

Milgram, S. (1967). *Small World Problem*.

MIT. (2016). What is System Dynamics? Retrieved November 23, 2016, from http://web.mit.edu/sysdyn/sd-intro/

Newman, M. E. J. (2002). Assortative Mixing in Networks. *Physical Review Letters*, *89*(20), 208701. https://doi.org/10.1103/PhysRevLett.89.208701

Newman, M. E. J. (2003). The structure and function of complex networks. *SIAM Review*, *45*(2), 167–256. https://doi.org/10.1137/S003614450342480

North, M. J. (2001). Smart II: The Spot Market Agent Research Tool version 2.0. *Natural Resources and Environmental Issues*, *8*(1), 11.

North, M. J. N. (2000). *SMART II+: the spot market agent research tool version 2.0 plus natural gas.* Argonne National Lab., IL (US). Retrieved from http://www.osti.gov/scitech/biblio/772131

Reed, D. A., Kapur, K. C., & Christie, R. D. (2009). Methodology for Assessing the Resilience of Networked Infrastructure. *IEEE Systems Journal*, *3*(2), 174–180. https://doi.org/10.1109/JSYST.2009.2017396

Rose, A. (1995). Input-output economics and computable general equilibrium models. *Structural Change and Economic Dynamics*, *6*(3), 295–304.

Rose, A., Oladosu, G., & Liao, S.-Y. (2007). Regional economic impacts of a terrorist attack on the water system of Los Angeles: A computable general disequilibrium analysis. Retrieved from https://books.google.ca/books?hl=en&lr=&id=wXkAAgAAQBAJ&oi=fnd&pg=PA291&dq=rose+regional+economic+impacts+of+terrorist+attacks&ots=nJ2K97ZxFf&sig=JQ9oCKL8Q5033LGgWKYl0saA0F4

Sachs, H., Stiebitz, M., & Wilson, R. J. (1988). An historical note: Euler's Königsberg letters. *Journal of Graph Theory, 12*(1), 133–139. https://doi.org/10.1002/jgt.3190120114

Santella, N., Zoli, C. B., & Steinberg, L. J. (2011). Baton Rouge Post-Katrina: The Role of Critical Infrastructure Modeling in Promoting Resilience. Retrieved from http://calhoun.nps.edu/handle/10945/25030

Santos, J. R. (2006). Inoperability input-output modeling of disruptions to interdependent economic systems. *Systems Engineering, 9*(1), 20–34. https://doi.org/10.1002/sys.20040

Santos, J. R., & Haimes, Y. Y. (2004). Modeling the Demand Reduction Input-Output (I-O) Inoperability Due to Terrorism of Interconnected Infrastructures*. *Risk Analysis, 24*(6), 1437–1451. https://doi.org/10.1111/j.0272-4332.2004.00540.x

Schneider, C. M., Moreira, A. A., Andrade, J. S., Havlin, S., & Herrmann, H. J. (2011). Mitigation of malicious attacks on networks. *Proceedings of the National Academy of Sciences, 108*(10), 3838–3841.

Schuster, A. (2008). Robust Artificial Neural Network Architectures. *ResearchGate*. Retrieved from

https://www.researchgate.net/publication/240704724_Robust_Artificial_Neural_Network_Architectures

Shannon, C. E. (1948). A Mathematical Theory of Communication. *Bell System Technical Journal*, *27*(3), 379–423. https://doi.org/10.1002/j.1538-7305.1948.tb01338.x

Singer, Y. (2016). Harvard University: CS 284r. Retrieved November 15, 2016, from http://people.seas.harvard.edu/~yaron/cs284r/

Sussman, G. J. (2008). Building Robust Systems an essay. *ResearchGate*. Retrieved from https://www.researchgate.net/publication/237249977_Building_Robust_Systems_an_essay

Taguchi, G., & Clausing, D. (1990, January 1). Robust Quality. Retrieved November 10, 2016, from https://hbr.org/1990/01/robust-quality

United States Air University. (2003). Al-Qaeda Training Manual. Retrieved from https://www.hsdl.org/?abstract&did=2046

Watts, D. J. (2016). US power grid - Network analysis of US power grid - KONECT. Retrieved November 12, 2016, from http://konect.uni-koblenz.de/networks/opsahl-powergrid

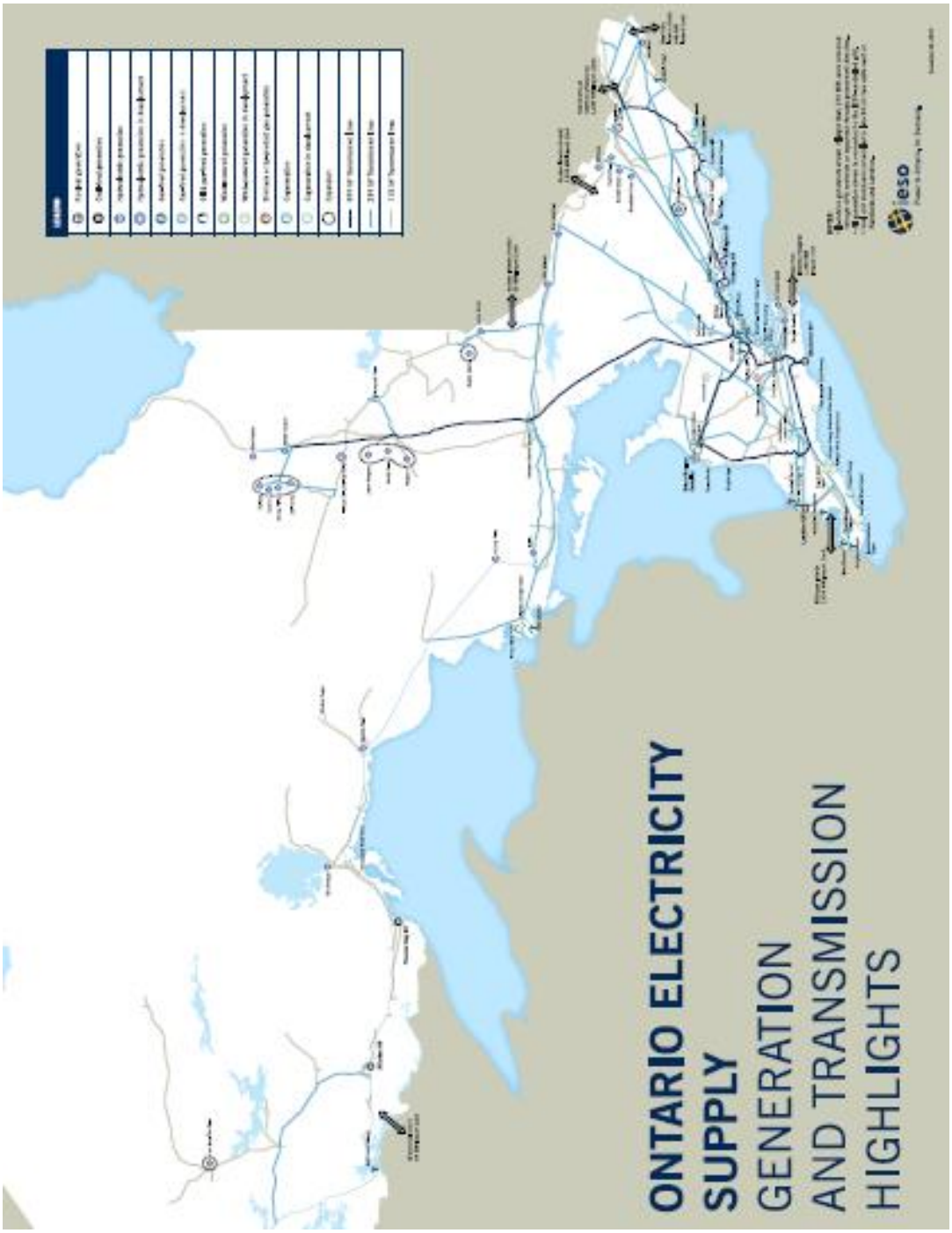
Watts, D. J., & Strogatz, S. H. (1998). Collective dynamics of "small-world" networks. *Nature*, *393*(6684), 440–442. https://doi.org/10.1038/30918

Wikipedia. (2016). Seven Bridges of Königsberg - Wikipedia, the free encyclopedia. Retrieved September 2, 2016, from https://en.wikipedia.org/wiki/Seven_Bridges_of_K%C3%B6nigsberg

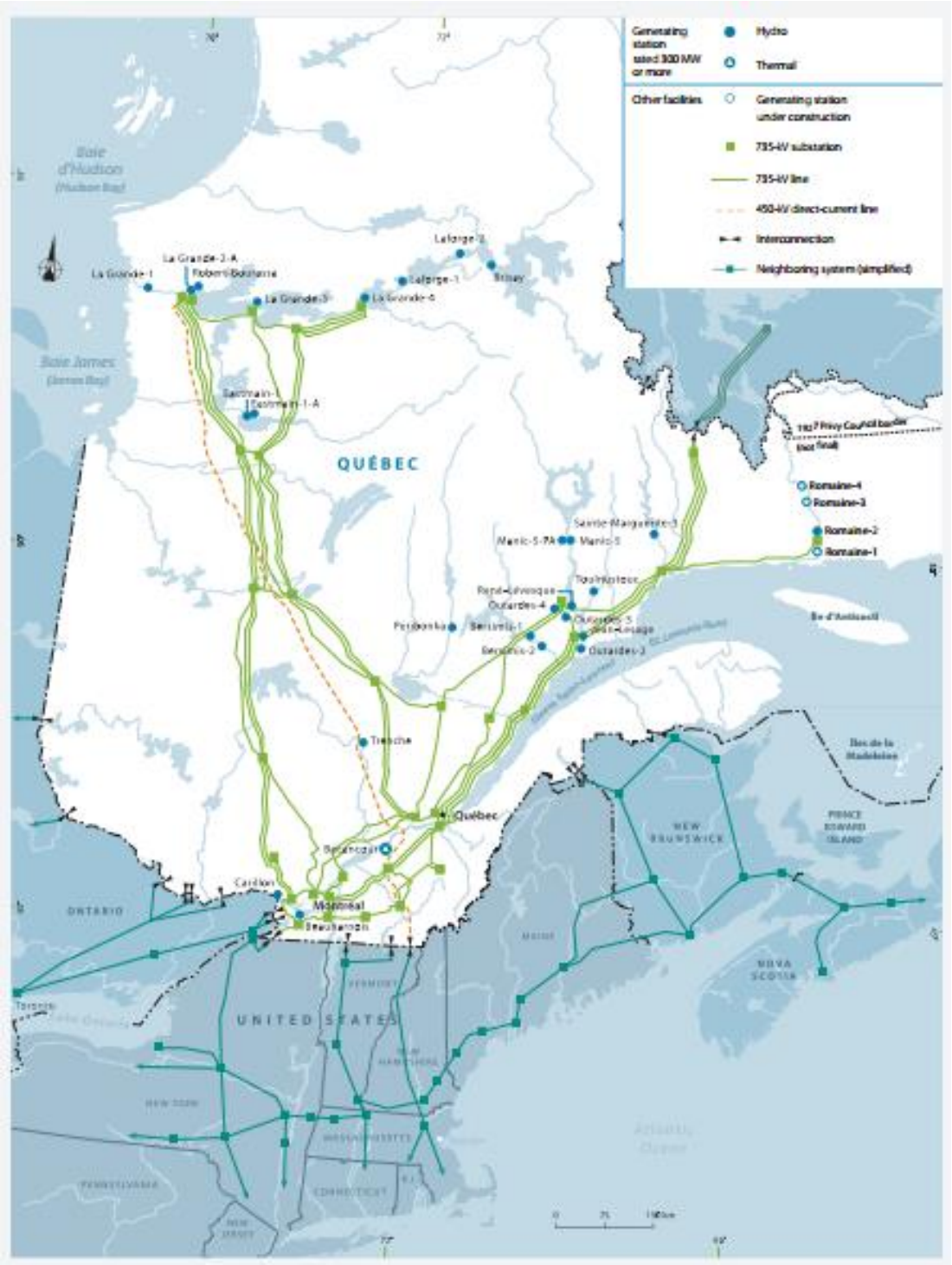
APPENDIX A – SYSTEM DIAGRAMS

1. British Columbia – System Diagram

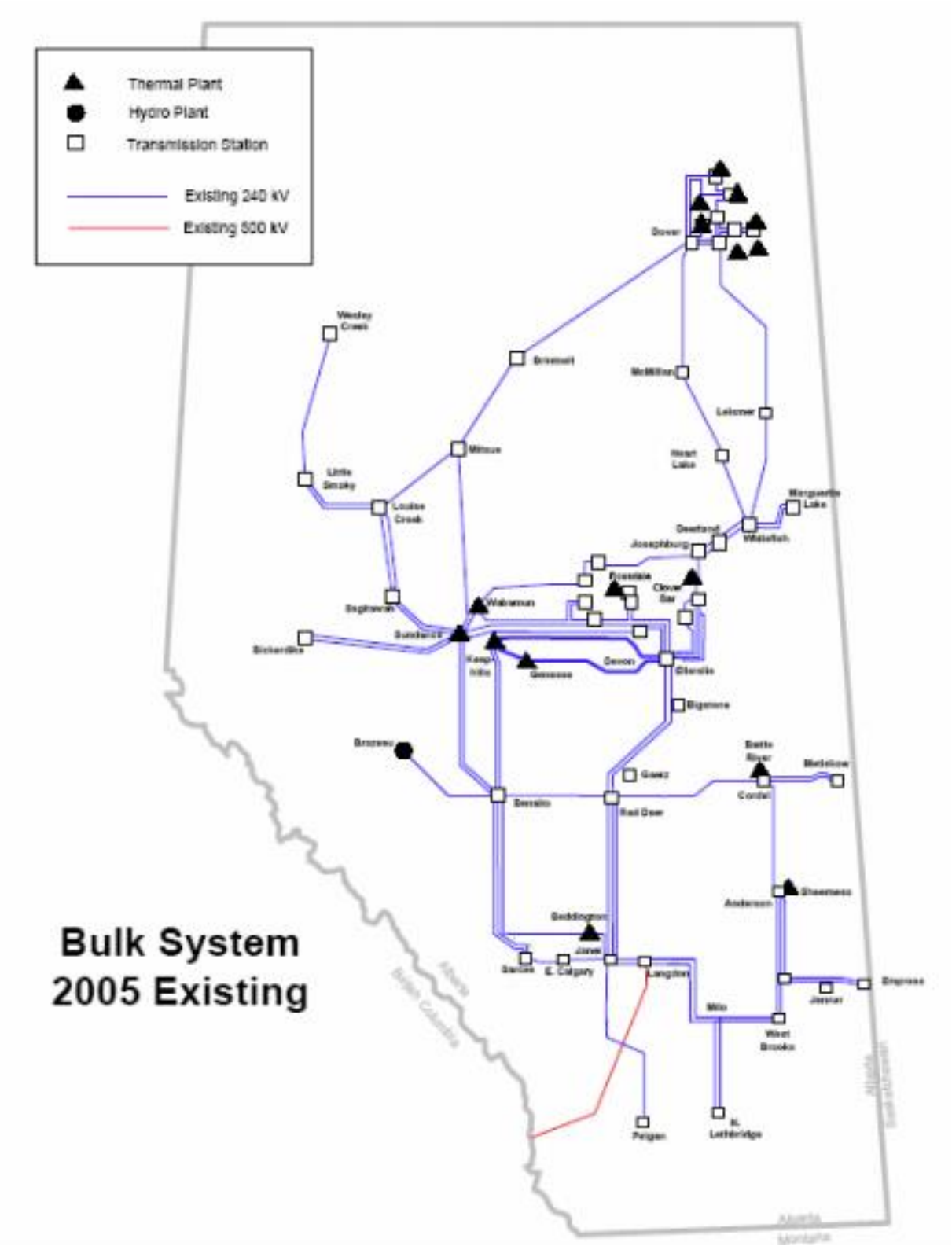
2. Ontario – System Diagram



3. Quebec – System Diagram



4. Alberta – System Diagram



APPENDIX B – CENTRALITY SCORES

1. British Columbia – Centrality Scores

nodeID	degree	betw	closeness	eigenvector	random
1	2	13.50	0.0062	0.0019	9
2	2	0.50	0.0053	0.0012	26
3	2	13.50	0.0062	0.0019	23
4	3	78.50	0.0074	0.0049	6
5	3	166.00	0.0088	0.0119	15
6	2	54.00	0.0072	0.0042	21
7	2	28.00	0.0061	0.0014	29
8	1	0.00	0.0052	0.0005	14
9	2	168.00	0.01	0.0289	24
10	4	216.50	0.0114	0.0805	16
11	3	44.50	0.009	0.0376	27
12	1	0.00	0.0072	0.0117	19
13	4	77.50	0.0104	0.0885	28
14	5	216.00	0.0114	0.1025	13
15	1	0.00	0.0086	0.032	8
16	2	4.00	0.0076	0.0279	17
17	3	11.50	0.0085	0.0516	2
18	3	28.00	0.0083	0.0486	22
19	2	76.00	0.01	0.0601	20
20	3	104.00	0.0102	0.0666	1
21	1	0.00	0.0079	0.0208	11
22	6	166.00	0.0091	0.0898	12
23	1	0.00	0.0072	0.0281	10
24	1	0.00	0.0072	0.0281	7
25	3	28.00	0.0075	0.0499	30
26	4	55.00	0.0076	0.0543	4
27	1	0.00	0.0062	0.0156	5
28	1	0.00	0.0063	0.017	18
29	1	0.00	0.0063	0.017	3
30	1	0.00	0.0068	0.0152	25

2. Ontario – Centrality Scores

nodeID	degree	betw	closeness	eigenvector	random
1	1	0.00	0.0013	0	14
2	1	0.00	0.0013	0	32
3	3	125.00	0.0014	0	8
4	4	245.00	0.0016	0	29
5	1	0.00	0.0014	0	28
6	3	343.00	0.0017	0	47
7	1	0.00	0.0015	0	61
8	2	5.00	0.0016	0	17
9	2	56.00	0.0017	0	44
10	3	497.00	0.0019	0	18
11	2	540.00	0.002	0.0001	2
12	3	583.00	0.0022	0.0002	49
13	3	63.00	0.0022	0.0002	12
14	1	0.00	0.0019	0.0001	52
15	3	700.00	0.0024	0.0005	55
16	4	830.00	0.0027	0.0013	53
17	1	0.00	0.0023	0.0004	65
18	1	0.00	0.0023	0.0004	38
19	4	874.00	0.0029	0.0033	33
20	1	0.00	0.0025	0.0009	50
21	2	820.00	0.0031	0.0056	59
22	2	40.00	0.0028	0.0037	4
23	3	882.00	0.0033	0.0164	46
24	3	63.00	0.0029	0.0099	35
25	5	1339.60	0.0035	0.0423	7
26	2	40.00	0.0031	0.0148	5
27	4	604.10	0.0031	0.0242	19
28	2	64.30	0.0023	0.0055	42
29	3	64.00	0.0021	0.0032	48
30	1	0.00	0.0018	0.0009	51
31	2	57.7	0.0023	0.0049	3
32	4	233.7	0.0027	0.014	9
33	2	63	0.0023	0.0043	26
34	1	0	0.002	0.0012	54
35	4	132.3	0.0027	0.0161	10
36	3	175.4	0.0027	0.013	60
37	4	137.7	0.0024	0.0055	25
38	1	0	0.002	0.0015	27

2. Ontario – Centrality Scores

nodeID	degree	betw	closeness	eigenvector	random
39	1	0	0.002	0.0015	39
40	2	17.9	0.0023	0.0032	36
41	2	62.3	0.0026	0.0058	22
42	3	173.6	0.003	0.0172	16
43	2	38.8	0.0026	0.0125	58
44	3	31.8	0.0025	0.0268	20
45	5	911.4	0.0033	0.0766	6
46	3	104.7	0.0028	0.0491	1
47	4	34.3	0.0025	0.0505	56
48	2	0	0.0022	0.0295	11
49	3	1.7	0.0024	0.046	15
50	5	233.7	0.0025	0.0534	45
51	3	125	0.0022	0.0181	34
52	1	0	0.0019	0.0051	37
53	1	0	0.0019	0.0051	64
54	4	318.3	0.0028	0.0626	30
55	2	15.5	0.0023	0.0279	13
56	3	72.5	0.0025	0.0448	63
57	5	417.8	0.0029	0.0677	62
58	3	37.8	0.0028	0.0485	23
59	3	65.7	0.0025	0.0336	21
60	4	234.7	0.0025	0.0351	41
61	3	50.2	0.0022	0.024	40
62	2	28	0.0022	0.0138	57
63	3	45.8	0.0022	0.0183	31
64	3	1.5	0.0019	0.0136	24
65	3	6.3	0.002	0.0158	43

3. Quebec – Centrality Scores

nodeID	degree	betw	closeness	eigenvector	random
1	1	0.00	0.0024	0.0006	59
2	1	0.00	0.0021	0.0002	16
3	1	0.00	0.0021	0.0002	30
4	3	117.00	0.0024	0.0007	47
5	4	239.77	0.0028	0.002	32
6	4	165.83	0.0028	0.0025	17
7	1	0.00	0.0024	0.0007	5
8	3	476.53	0.0032	0.0029	2
9	3	377.00	0.0028	0.001	31
10	1	0.00	0.0024	0.0003	33
11	3	279.00	0.0025	0.0004	49
12	1	0.00	0.0022	0.0001	6
13	3	173.00	0.0022	0.0001	48
14	1	0.00	0.0019	0	12
15	2	59.00	0.0019	0	34
16	1	0.00	0.0017	0	22
17	3	196.85	0.003	0.0032	36
18	2	1.00	0.0028	0.0018	52
19	3	94.62	0.0031	0.0031	35
20	3	318.88	0.0034	0.0073	38
21	4	595.32	0.0036	0.0067	13
22	3	401.92	0.0037	0.0158	28
23	3	549.78	0.0038	0.0102	57
24	2	459.58	0.0038	0.0132	19
25	4	384.97	0.0038	0.0379	20
26	4	503.58	0.0039	0.0362	61
27	1	0.00	0.0032	0.0103	11
28	4	532.67	0.0038	0.0474	60
29	1	0.00	0.0031	0.0135	24
30	2	0.00	0.0032	0.0229	43
31	5	350.7722	0.004	0.056	45
32	4	363.0583	0.0039	0.0517	46
33	5	181.45	0.0036	0.0425	37
34	1	0	0.0029	0.0121	56
35	3	96.5667	0.0032	0.0243	3
36	1	0	0.0027	0.0069	27
37	4	82.0667	0.0031	0.036	54
38	4	168.7444	0.0034	0.0449	14
39	2	3.8611	0.0026	0.0161	18
40	3	21.3611	0.0027	0.0204	41

3. Quebec – Centrality Scores

nodeID	degree	betw	closeness	eigenvector	random
41	5	180.2	0.0032	0.0409	1
42	2	21.2083	0.0034	0.0288	53
43	1	0	0.0027	0.0117	26
44	2	15.25	0.0027	0.0145	51
45	4	179.9722	0.0032	0.0306	25
46	3	125.8139	0.0035	0.0322	4
47	2	27.125	0.0032	0.0265	8
48	8	554.9167	0.0035	0.0607	44
49	1	0	0.0029	0.0173	42
50	1	0	0.0029	0.0173	9
51	1	0	0.0029	0.0173	29
52	1	0	0.0029	0.0173	21
53	2	88.7917	0.0029	0.0196	10
54	5	195.5417	0.0031	0.0381	58
55	1	0	0.0026	0.0109	15
56	1	0	0.0026	0.0109	50
57	3	224	0.003	0.0315	23
58	4	174	0.0026	0.0119	39
59	1	0	0.0023	0.0034	55
60	1	0	0.0023	0.0034	7
61	1	0	0.0023	0.0034	40

4. Alberta – Centrality Scores

nodeID	degree	betw	closeness	eigenvector	random
1	1	0.00	0.0033	0.0009	5
2	2	47.00	0.0039	0.0034	44
3	3	95.80	0.0047	0.0122	31
4	3	247.48	0.0058	0.0223	16
5	2	161.06	0.0049	0.0066	29
6	2	54.75	0.0053	0.0206	28
7	7	542.02	0.0068	0.066	41
8	1	0.00	0.0052	0.0174	14
9	3	125.01	0.0056	0.0251	22
10	2	64.92	0.0048	0.0074	21
11	2	42.17	0.0043	0.0029	2
12	3	53.92	0.0049	0.0221	46
13	1	0.00	0.004	0.0058	9
14	4	120.83	0.006	0.0532	40
15	3	47.00	0.005	0.0369	36
16	1	0.00	0.004	0.0097	24
17	3	99.69	0.0041	0.0035	35
18	4	88.75	0.0037	0.0017	49
19	1	0.00	0.0031	0.0005	18
20	2	20.66	0.0038	0.0012	25
21	4	133.39	0.0043	0.0027	47
22	3	29.57	0.0038	0.0015	20
23	2	0.00	0.0037	0.0011	17
24	2	80.93	0.0044	0.0088	8
25	8	237.10	0.0058	0.0773	42
26	2	0.00	0.0048	0.0283	6
27	3	107.93	0.005	0.0301	27
28	2	27.42	0.0057	0.0377	10
29	3	97.44	0.0058	0.0487	38
30	2	0.00	0.005	0.0331	34
31	2	50.5778	0.0053	0.0259	1
32	2	50.2444	0.0052	0.0212	4
33	5	350.0556	0.0059	0.0548	23
34	6	498.0889	0.0067	0.0747	48
35	1	0	0.0051	0.0196	32
36	4	81.4444	0.0057	0.0551	15
37	3	32.5	0.0053	0.0397	26
38	2	2.75	0.0046	0.021	7

4. Alberta – Centrality Scores

nodeID	degree	betw	closeness	eigenvector	random
39	5	173.5	0.0049	0.0403	30
40	1	0	0.004	0.0106	11
41	2	84	0.0041	0.0117	12
42	3	55	0.0036	0.004	37
43	1	0	0.0031	0.0011	3
44	2	13	0.0036	0.0025	19
45	3	134	0.0042	0.0056	13
46	2	47	0.0035	0.0016	43
47	1	0	0.003	0.0004	39
48	3	203	0.0049	0.0171	45
49	1	0	0.004	0.0045	33